

## DeviceLock DLP 9.0

### Update 4

# Table of contents

<b>DeviceLock Overview</b>	<b>12</b>
General Information	12
Managed Access Control	15
DeviceLock Service for Mac	20
DeviceLock Content Security Server	21
How Search Server Works	22
Indexing DeviceLock Enterprise Server Data	22
Executing Search Queries	23
ContentLock and NetworkLock	23
ContentLock and NetworkLock Licensing	28
User Activity Monitor (UAM)	29
UAM Licensing	30
Basic Security Rules	31
<b>Installing DeviceLock</b>	<b>33</b>
System Requirements	33
Deploying DeviceLock Service for Windows	36
Interactive Installation	37
Unattended Installation	43
Installation via Microsoft Systems Management Server	45
Installation via DeviceLock Management Console	45
Installation via DeviceLock Enterprise Manager	45
Installation via Group Policy	47
Installation via DeviceLock Enterprise Server	54
Deploying DeviceLock Service for Mac	56
Interactive Installation	56
Command Line Utility	59
Unattended Installation	59
Installing Management Consoles	60
Installing DeviceLock Enterprise Server	64
Installation Steps	65
Installing DeviceLock Content Security Server	80
Prepare to Install	80
Start Installation	82
Perform Configuration and Complete Installation	83
<b>DeviceLock Consoles and Tools</b>	<b>96</b>

DeviceLock Management Console .....	96
Interface .....	97
Connecting to Computers .....	99
DeviceLock Service Settings Editor .....	103
Creating or Modifying a Policy .....	105
DeviceLock Group Policy Manager .....	106
How Group Policy is applied .....	107
Standard GPO inheritance rules .....	107
Recommendations .....	108
Getting started with DeviceLock Group Policy Manager .....	108
Using DeviceLock Group Policy Manager .....	111
Using Resultant Set of Policy (RSOP) .....	114
Using Group Policy to Manage DeviceLock Service for Mac .....	116
DeviceLock Enterprise Manager .....	116
Interface .....	117
Scan Network Dialog Box .....	119
Plug-ins .....	128
Open / Save / Export .....	134
Comparing Data .....	135
Filtering Data .....	140
DeviceLock Certificates .....	142
Generating DeviceLock Certificates .....	143
Installing/Removing DeviceLock Certificate .....	145
DeviceLock Signing Tool .....	148
Device Code .....	149
Service Settings .....	150
<b>DeviceLock Service .....</b>	<b>157</b>
Managing DeviceLock Service for Windows .....	157
Service Options .....	158
Devices Node .....	216
Permissions (Regular Profile) .....	217
Auditing, Shadowing & Alerts (Regular Profile) .....	228
USB Devices White List (Regular Profile) .....	241
Media White List (Regular Profile) .....	248
Security Settings (Regular Profile) .....	254
Audit Log Viewer (Service) .....	258
Shadow Log Viewer (Service) .....	265

Managing DeviceLock Service for Mac .....	274
Enabling NTLM authentication for local users on Mac OS X .....	275
<b>Content-Aware Rules (Regular Profile) .....</b>	<b>280</b>
Rules for Devices .....	280
Content-Aware Rules Node .....	281
Access Control .....	283
Content-Aware Shadowing .....	288
Content-Aware Detection .....	291
Rules for Protocols .....	293
Content-Aware Rules Node .....	294
Access Control .....	296
Content-Aware Shadowing .....	300
Content-Aware Detection .....	303
Configuring Content Groups .....	307
File Type Detection Content Groups .....	307
Keywords Content Groups .....	312
Pattern Content Groups .....	319
Document Properties Content Groups .....	326
Complex Content Groups .....	334
Viewing Built-in Content Groups .....	337
Duplicating Built-in Content Groups .....	338
Editing or Deleting Custom Content Groups .....	338
Testing Content Groups .....	339
Managing Content-Aware Rules .....	340
Defining Content-Aware Rules .....	340
Editing Content-Aware Rules .....	349
Copying Content-Aware Rules .....	350
Exporting and Importing Content-Aware Rules .....	351
Undefining Content-Aware Rules .....	353
Deleting Content-Aware Rules .....	353
<b>Digital Fingerprints .....</b>	<b>355</b>
Digital Fingerprinting Technique .....	355
How It Works .....	355
Fingerprints Collection and Storage .....	357
About Versioning Threshold .....	358
Fingerprints Matching .....	359
What If Server's Fingerprints Database Is Unavailable to Client? .....	359



Getting Started Using Digital Fingerprints .....	360
Administering Digital Fingerprints .....	360
Fingerprinting Options .....	361
Fingerprinting Tasks .....	362
Fingerprints Database .....	367
Fingerprints Log Viewer .....	373
Applying Digital Fingerprints .....	377
Service Options for Digital Fingerprints .....	377
Digital Fingerprints Content Groups .....	379
<b>Protocols (Regular Profile) .....</b>	<b>382</b>
Overview .....	382
Protocols Node .....	388
Managing Permissions for Protocols .....	389
Access Rights .....	389
Default Permissions .....	395
Permission Management Tasks .....	397
Managing Audit, Shadowing and Alerts for Protocols .....	401
Audit and Shadowing Rights .....	401
Default Audit and Shadowing .....	417
Auditing, Shadowing and Alerts Management Tasks .....	420
Managing Protocols White List .....	425
White List Rules .....	425
White List Rule Parameters .....	426
White List Management Tasks .....	433
Managing Basic IP Firewall .....	441
Firewall Rules .....	442
Firewall Rule Parameters .....	442
Firewall Management Tasks .....	445
Managing Security Settings for Protocols .....	453
Security Settings Description .....	454
Security Settings Management Tasks .....	455
Inspection and Control of SSL-encrypted Traffic .....	457
<b>DeviceLock Security Policies (Offline Profile) .....</b>	<b>459</b>
Overview .....	459
Configuring Offline Mode Detection Settings .....	460
Switching Between Online and Offline Mode .....	462
Managing Offline Security Policies for Devices .....	462

Managing Offline Permissions for Devices .....	463
Managing Offline Audit, Shadowing and Alerts for Devices .....	467
Managing Offline USB Devices White List .....	472
Managing Offline Media White List .....	479
Managing Offline Content-Aware Rules for Devices .....	485
Managing Offline Security Settings for Devices .....	495
Managing Offline Security Policies for Protocols .....	500
Managing Offline Permissions for Protocols .....	500
Managing Offline Audit, Shadowing and Alerts for Protocols .....	504
Managing Offline Protocols White List .....	509
Managing Offline IP Firewall .....	518
Managing Offline Content-Aware Rules for Protocols .....	527
Managing Offline Security Settings for Protocols .....	538
<b>Temporary White List .....</b>	<b>541</b>
Overview .....	541
Temporary White List Authorization Tool .....	542
<b>User Activity Monitor .....</b>	<b>545</b>
Introduction to User Activity Monitor .....	545
Getting Started with User Activity Monitor .....	545
Monitoring Settings .....	546
Options .....	547
Rules .....	549
Viewing User Activity .....	565
List of Monitoring Sessions .....	566
Session Viewer .....	568
Managing the UAM Log .....	570
<b>DeviceLock Enterprise Server .....</b>	<b>575</b>
Administering DeviceLock Enterprise Server .....	575
Server Options .....	576
Using Log Viewers .....	578
Audit Log Viewer (Server) .....	578
Shadow Log Viewer (Server) .....	585
Server Log Viewer .....	593
Consolidating Logs .....	599
Getting Started Using the Consolidation of Logs .....	599
Administering the Consolidation of Logs .....	600
Monitoring .....	604

Monitoring Tasks .....	605
Monitoring Log Viewer .....	616
<b>DeviceLock Enterprise Server Policies .....</b>	<b>623</b>
Overview .....	623
How Policies Are Processed and Applied .....	623
Policy Application Scenarios: Required Configuration Steps .....	624
Managing DeviceLock Policies .....	626
Using the Policies Node .....	627
Managing Policy Objects .....	631
Managing Computers Assigned to Policy Objects .....	634
Using the Policy Log Viewer .....	636
<b>DeviceLock Reports .....</b>	<b>643</b>
Report Categories and Types .....	643
Relations Charts .....	644
User Dossiers .....	650
Audit Log Reports .....	665
Shadow Log Reports .....	675
Report Creation Tasks .....	682
Creating Tasks .....	683
Managing Existing Tasks .....	695
Viewing Reports Created by a Task .....	696
Configuring E-mail Delivery of Reports .....	698
Setting Default Format for Reports .....	699
Working with Reports .....	699
Generating Reports .....	700
Refreshing Lists of Reports .....	700
Viewing Reports .....	701
Viewing Report Parameters .....	701
Exporting and Saving Reports .....	701
Sending Reports by E-mail .....	702
Deleting Reports .....	703
<b>DeviceLock Content Security Server .....</b>	<b>704</b>
Administering DeviceLock Content Security Server .....	704
Server Options .....	705
Managing General Settings .....	706
Managing Search Server Settings .....	712
Using Search Server .....	719

Performing a search .....	720
About logical operators .....	723
AND/OR operators .....	723
Working with search results .....	738
Automating search operations .....	748
File Formats Indexed for Search .....	761
<b>Appendix: Activating DeviceLock Licenses .....</b>	<b>764</b>
About DeviceLock License Types .....	764
Activating Client Licenses .....	765
Activating Server Licenses .....	766
Enterprise Server .....	766
Search Server .....	767
Discovery Server .....	767
<b>Appendix: Consolidating the Logs in the Cloud Using OpenVPN .....</b>	<b>768</b>
Requirements Overview .....	768
Configuring the Cloud Server .....	769
Install OpenVPN .....	769
Prepare the Server Certificates .....	769
Configure the OpenVPN Server .....	770
Configure the DeviceLock Enterprise Server .....	771
Configuring On-premises Servers .....	772
Install OpenVPN .....	772
Prepare the Client Certificate and IP Address .....	772
Configure the OpenVPN Client .....	774
Configure the DeviceLock Enterprise Server .....	775
Test: Connect the Console to the Cloud Server .....	775
<b>Appendix: Examples .....</b>	<b>777</b>
Permission and Audit Examples for Devices .....	777
Permission Examples .....	777
Audit & Shadowing Examples .....	791
Permission Examples for Protocols .....	794
Content-Aware Rule Examples .....	797
Basic IP Firewall Rule Examples .....	802
<b>DeviceLock Discovery Overview .....</b>	<b>805</b>
Introducing DeviceLock Discovery .....	805
Understanding DeviceLock Discovery .....	805
Features and Benefits .....	805

How DeviceLock Discovery Works .....	809
Licensing .....	811
<b>Installing DeviceLock Discovery .....</b>	<b>812</b>
Installing DeviceLock Content Security Server .....	812
Prepare to Install .....	812
Start Installation .....	813
Perform Configuration and Complete Installation .....	814
<b>Setting Up Discovery Server .....</b>	<b>827</b>
Navigating Discovery Server .....	827
General Settings .....	829
Configuring access to the DeviceLock Content Security Server .....	830
Setting the service startup account .....	832
Installing or removing a DeviceLock certificate .....	833
Configuring the TCP Port setting .....	833
Managing the database connection settings .....	834
Discovery Server Options .....	834
Specifying Digital Fingerprints Database Server(s) .....	835
Installing DeviceLock Discovery licenses .....	836
Configuring log options .....	836
Setting up alert and notification messages .....	837
Setting the data collection interval .....	841
Enabling binary files content inspection .....	841
Alerts .....	842
General Information .....	842
Alerts Settings: SNMP .....	843
Alerts Settings: SMTP .....	846
Alerts Settings: Syslog .....	849
Alerts Settings: Delivery retry parameters .....	850
Resetting Alert Settings to Defaults .....	852
Resetting Individual Settings .....	852
<b>Endpoint Scanning .....</b>	<b>853</b>
Discovery Server .....	853
Units .....	853
Creating a Unit .....	854
Adding Filters .....	861
Managing Units .....	865
Elasticsearch Units .....	868

Rules and Actions .....	872
Rules & Actions Node .....	872
Defining and Editing Rules and Actions .....	874
Importing and Exporting Rules .....	880
Tasks .....	881
Tasks Node .....	882
Creating a Task .....	884
Task and Its Reports .....	887
Viewing a Report .....	889
Navigating Reports .....	893
Discovery results .....	893
Failed to scan .....	894
Details table .....	894
Rules .....	895
Links to the log viewer .....	895
Tasks Log Viewer .....	895
Managing the Tasks Log .....	897
Discovery Log Viewer .....	902
Managing the Discovery Log .....	903
<b>Index .....</b>	<b>907</b>

# Copyright statement

© Acronis International GmbH, 2003-2024. All rights reserved.

All trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at <https://kb.acronis.com/content/7696>

## Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

# DeviceLock Overview

## General Information

Preventing unauthorized downloading as well as the uploading of inappropriate software and data is important when trying to protect and administer a company's computer network.

DeviceLock DLP is easy to install. Administrators can have instant access from remote computers when necessary. The administrator of the machine or domain can designate user access to printers, clipboard, iPhones and iPads, floppy drives, optical drives, other removable media, tape drives, Media Transfer Protocol (MTP), WiFi, and Bluetooth adapters, or USB, FireWire, infrared, serial and parallel ports. All types of file systems are supported.

DeviceLock DLP provides control over network communications. Administrators can designate user access to the FTP, HTTP, IBM Notes, SMB, SMTP, MAPI (Microsoft Exchange), Telnet and Torrent protocols, instant messengers (Skype, Telegram, Viber, WhatsApp, ICQ Messenger, Jabber, IRC, Mail.ru Agent), cloud storages (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive, etc.), Web Mail and social networking applications (ABV Mail, AOL Mail, freenet.de, Gmail, GMX Mail, Hotmail (Outlook.com), iCloud, Mail.ru, NAVER, Outlook Web App (OWA), Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail, Zimbra; Facebook, Google+, Instagram, LinkedIn, LiveJournal, Myspace, Odnoklassniki, Pinterest, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru).

DeviceLock extracts and filters the content of data copied to removable drives and plug-n-play storage devices, as well as that transmitted over the network. Administrators can create rules that specify which content can be copied and transmitted.

DeviceLock can audit user activity for a particular device type or protocol on a local computer. Based on the user's security context, this capability allows you to audit activities that belong to a certain user or user group. DeviceLock employs the standard event logging subsystem and writes audit records to the Windows event log.

DeviceLock can generate real-time security alerts when significant incidents, events or problems occur. Real-time alerting simplifies event monitoring and log management and helps you response faster and more efficiently to security incidents and policy violations. Alerts are available via Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP) and syslog.

DeviceLock supports data shadowing - the ability to mirror all data copied to external storage devices, transferred through serial and parallel ports or transmitted over the network. A full copy of the files can be saved into the SQL database. Shadowing, like auditing, can be defined on a per-user basis.

Moreover, the DeviceLock data shadowing function is compatible with the National Software Reference Library maintained by the National Institute of Standards and Technology (NIST) and with the Hashkeeper Database designed and maintained by U.S. DOJ National Drug Intelligence Center (NDIC).



The data logged by DeviceLock can be checked against hash databases (collections of digital signatures of known, traceable data) and used in computer forensics.

You may also create your own database with digital signatures (SHA-1, MD5 and CRC32 are supported) of critical files and then use it for tracing purposes. For example, you can trace which users are copying signed files, at what time, and with which devices.

For information on how to use hash databases in cooperation with DeviceLock, please contact our technical support team.

More information about hash databases and their samples can be found on the National Software Reference Library's Web site at [www.nsrll.nist.gov](http://www.nsrll.nist.gov).

Also, DeviceLock provides instant searching of text across shadowed files and audit logs stored in the centralized database. DeviceLock can automatically recognize, index, search and display documents in many formats, such as: Adobe Acrobat (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (PDF), Ami Pro, AutoCAD (DWG, DXF), Archives (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Visio, Microsoft Word, Microsoft Works, OpenOffice (documents, spreadsheets and presentations), Quattro Pro, WordPerfect, WordStar and many others.

---

**Note**

Content in AutoCAD (DWG, DXF) file formats can be identified on Windows XP and later systems.

---

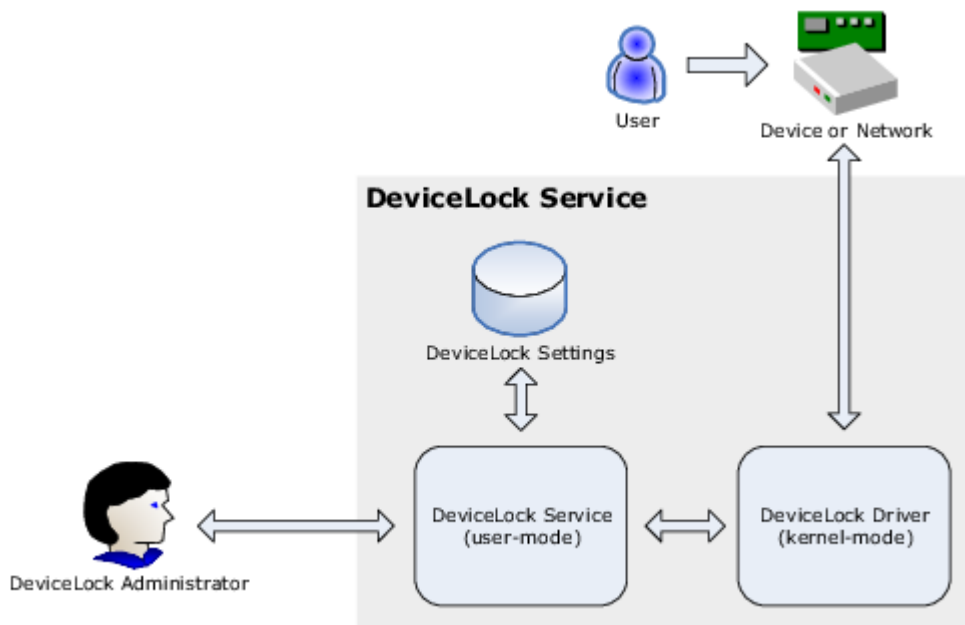
In addition to the standard (per computer) way of managing permissions, DeviceLock also provides you with a more powerful mechanism - permissions and settings can be changed and deployed via Group Policy in an Active Directory domain.

Tighter integration into the Active Directory is a very important function of DeviceLock. It makes DeviceLock's permissions management and deployment easier for large networks and more convenient for system administrators.

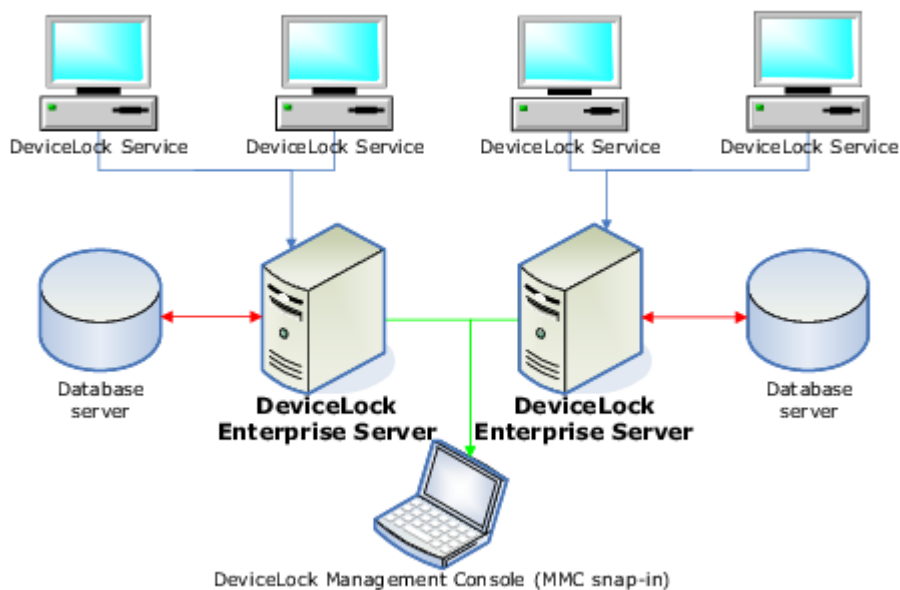
Integration into the Active Directory eliminates the need to install more third-party applications for centralized management and deployment. DeviceLock does not need to have its own server-based version to control the entire network, instead it uses standard functions provided by the Active Directory.

DeviceLock DLP consists of three parts: the agent (DeviceLock Service), servers (DeviceLock Enterprise Server and DeviceLock Content Security Server), and management consoles (DeviceLock Management Console, DeviceLock Group Policy Manager, and DeviceLock Enterprise Manager).

1. DeviceLock Service is the core of DeviceLock. DeviceLock Service is installed on each client system, runs automatically, and provides device and network protection on the client machine while remaining invisible to that computer's local users.

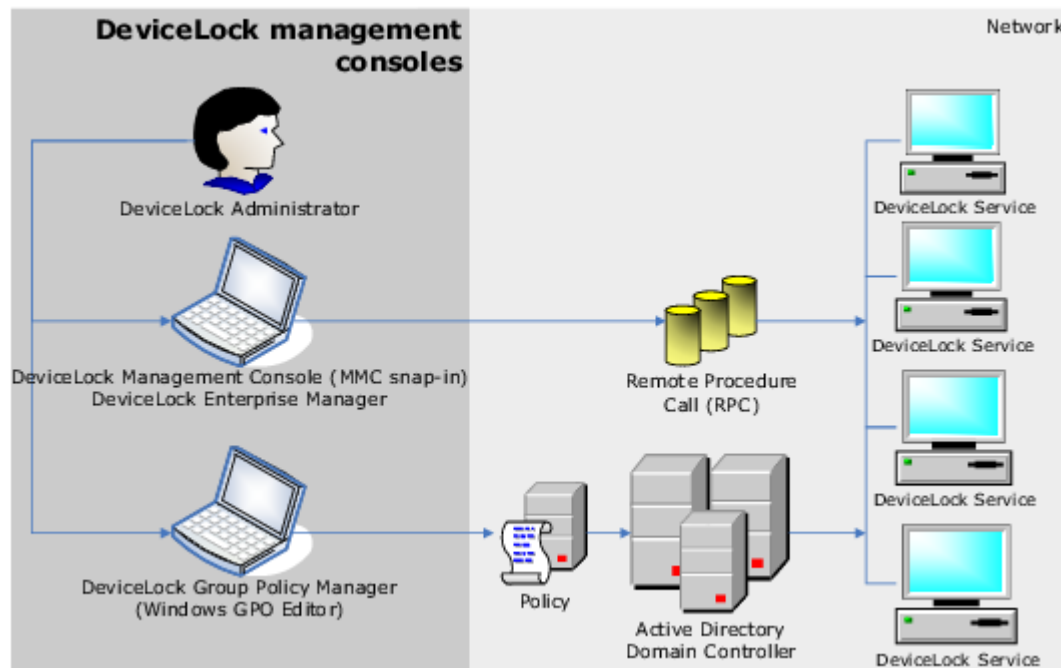


2. DeviceLock Enterprise Server (DLES) is an optional component for centralized collection and storage of the shadow data and audit logs. DeviceLock Enterprise Server uses a database server (SQL Server or PostgreSQL) to store its data. You can install several DLES instances and database servers to balance the network load.



DeviceLock Content Security Server is another optional component which includes Search Server for instant search of text within shadowed files and other logs stored on DeviceLock Enterprise Server. For more information, see [DeviceLock Content Security Server](#) later in this chapter.

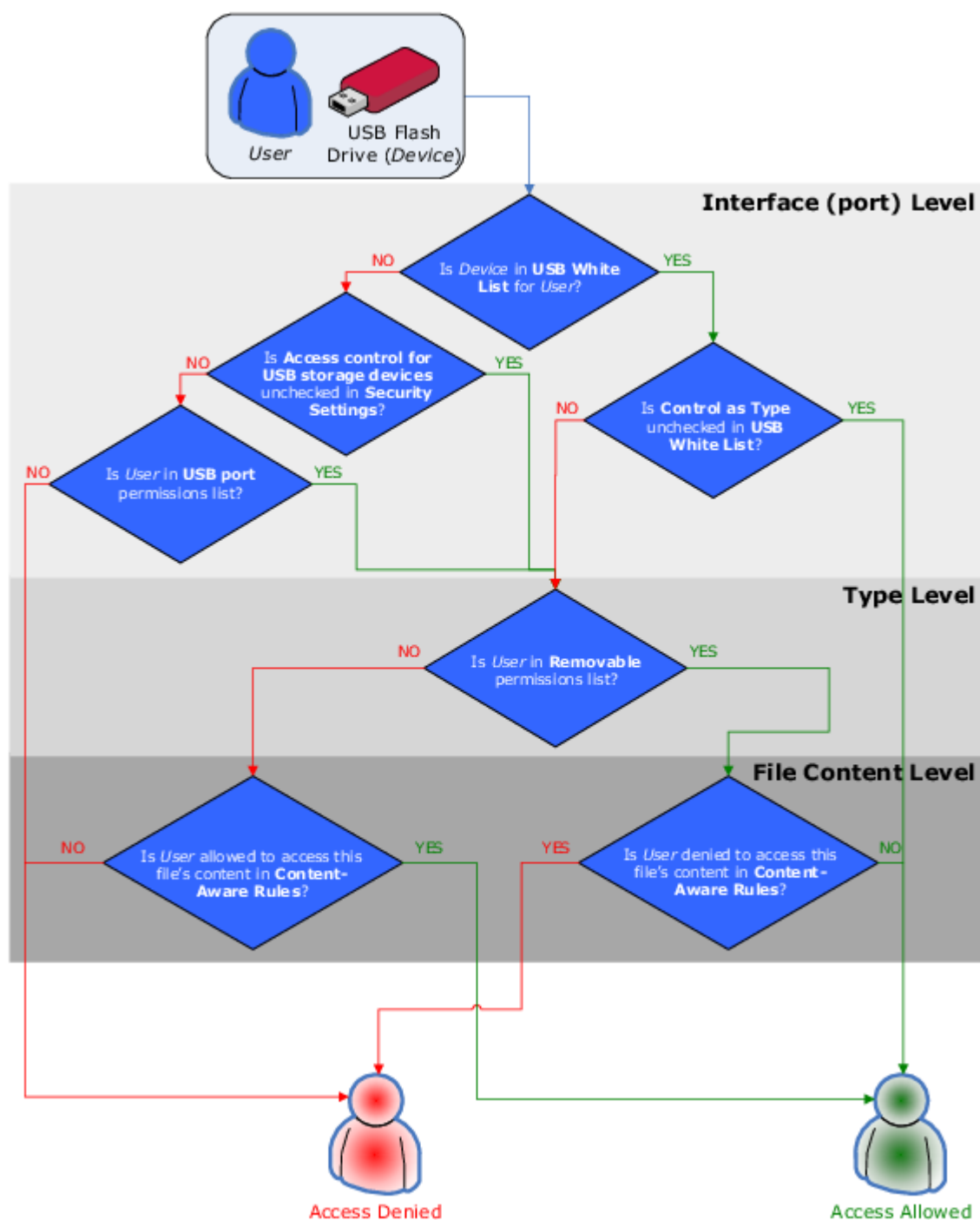
3. The management console is the control interface that systems administrators use to remotely manage each system that has DeviceLock Service. DeviceLock ships with four different management consoles: DeviceLock Management Console, DeviceLock Enterprise Manager, and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor). DeviceLock Management Console is also used to manage DeviceLock Enterprise Server and DeviceLock Content Security Server.



## Managed Access Control

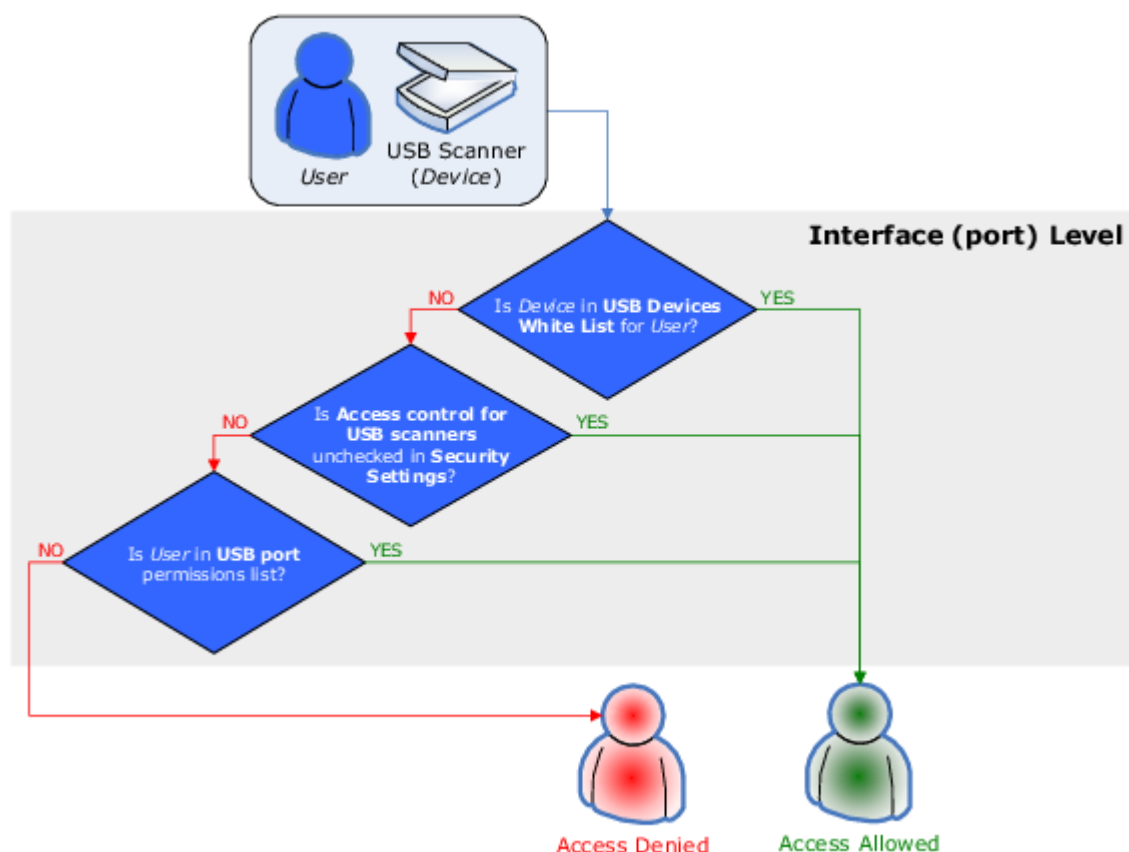
Access control for devices works in the following way: Every time the user wants to access a device, DeviceLock intercepts this request at the kernel level of the OS. Depending on the device's type and the connection interface (e.g. USB), DeviceLock checks the user rights in the appropriate Access Control List (ACL). If the user does not have the right to access this device, an "access denied" error is returned.

Access checking can occur at three levels: the interface (port) level, the type level and the file content level. Some devices are checked at all three levels, while others only at one level - either interface (port) or type.



Consider the case of a user connecting a USB flash drive to the USB port. Here DeviceLock would first check whether the USB port is open or locked at the interface level. Next, because Windows recognizes a USB flash drive as a removable storage device, DeviceLock will also check permissions at the type level (Removable). Finally, DeviceLock will also check permissions at the file content level (Content-Aware Rules).

In contrast, a USB scanner would only be checked at the interface level (USB port), as DeviceLock doesn't distinguish scanners at the type level.



There are additional security settings (see [Security Settings \(Regular Profile\)](#)) that can turn off access control for classes of devices (for example, all USB printers) while others remain under control. In the case of a device belonging to a class for which control is disabled, DeviceLock allows all requests to connect this device at the interface (port) level.

Also, DeviceLock supports the white listing of specific devices (see [USB Devices White List \(Regular Profile\)](#)); in other words, you can turn off access control for only specific devices (for example, certain USB printer).

---

#### Note

If access to a device is denied at the interface (port) level, DeviceLock does not check permissions at the type level. However, if access is granted at the interface (port) level, DeviceLock also checks permissions at the type level. Only when access is granted at both levels, the user can connect the device.

---

Access control for protocols works in the following way: Every time the user wants to access a remote network resource, DeviceLock intercepts this connection request at the kernel level of the OS and checks the user rights in the appropriate Access Control List (ACL). If the user does not have the right to access this protocol, an “access denied” error is returned.

---

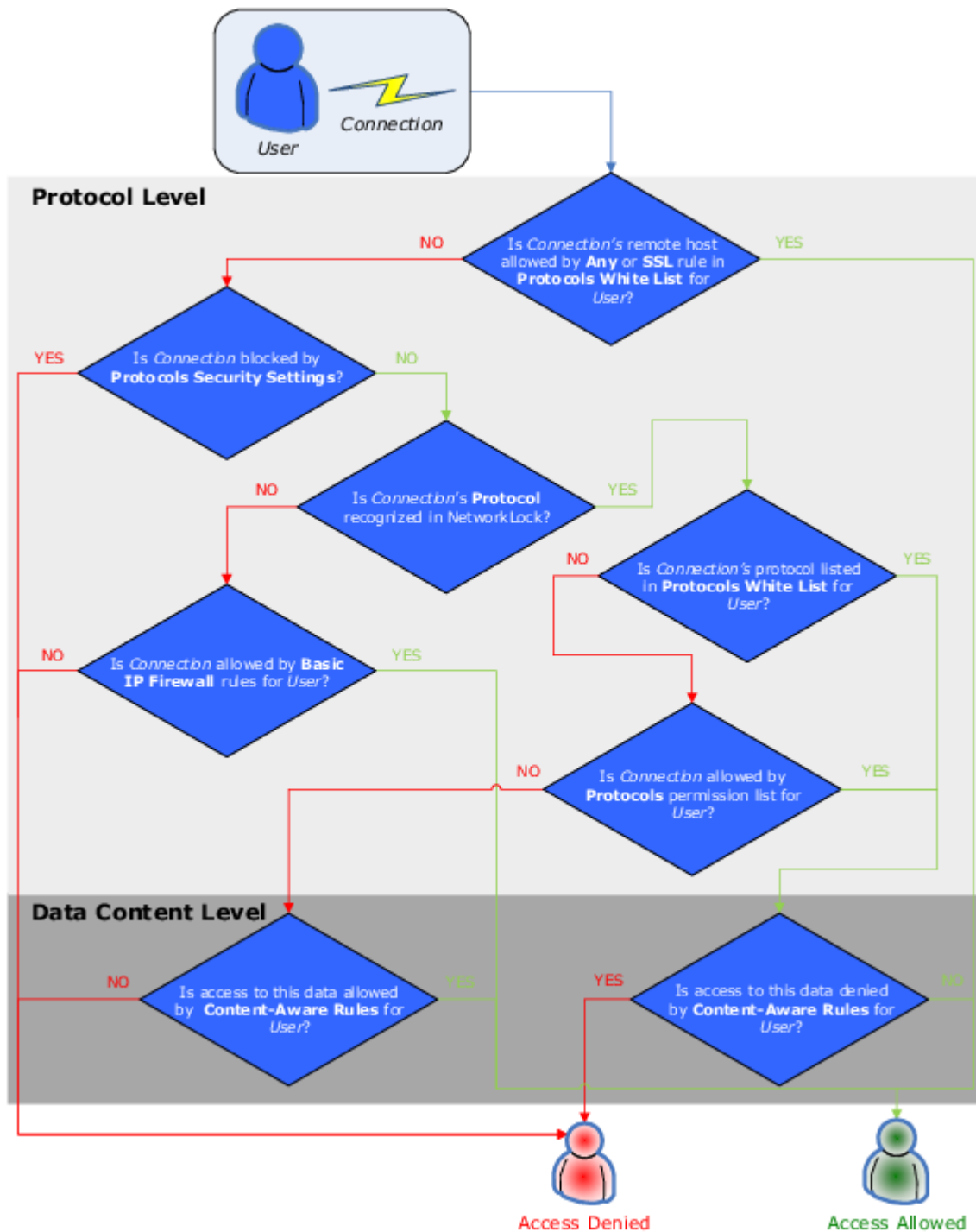
**Note**

Access control settings for Social Networks, File Sharing and Web Mail override access control settings for HTTP. For example, if users are allowed to access Gmail, but disallowed to use HTTP, they nevertheless can access the service.

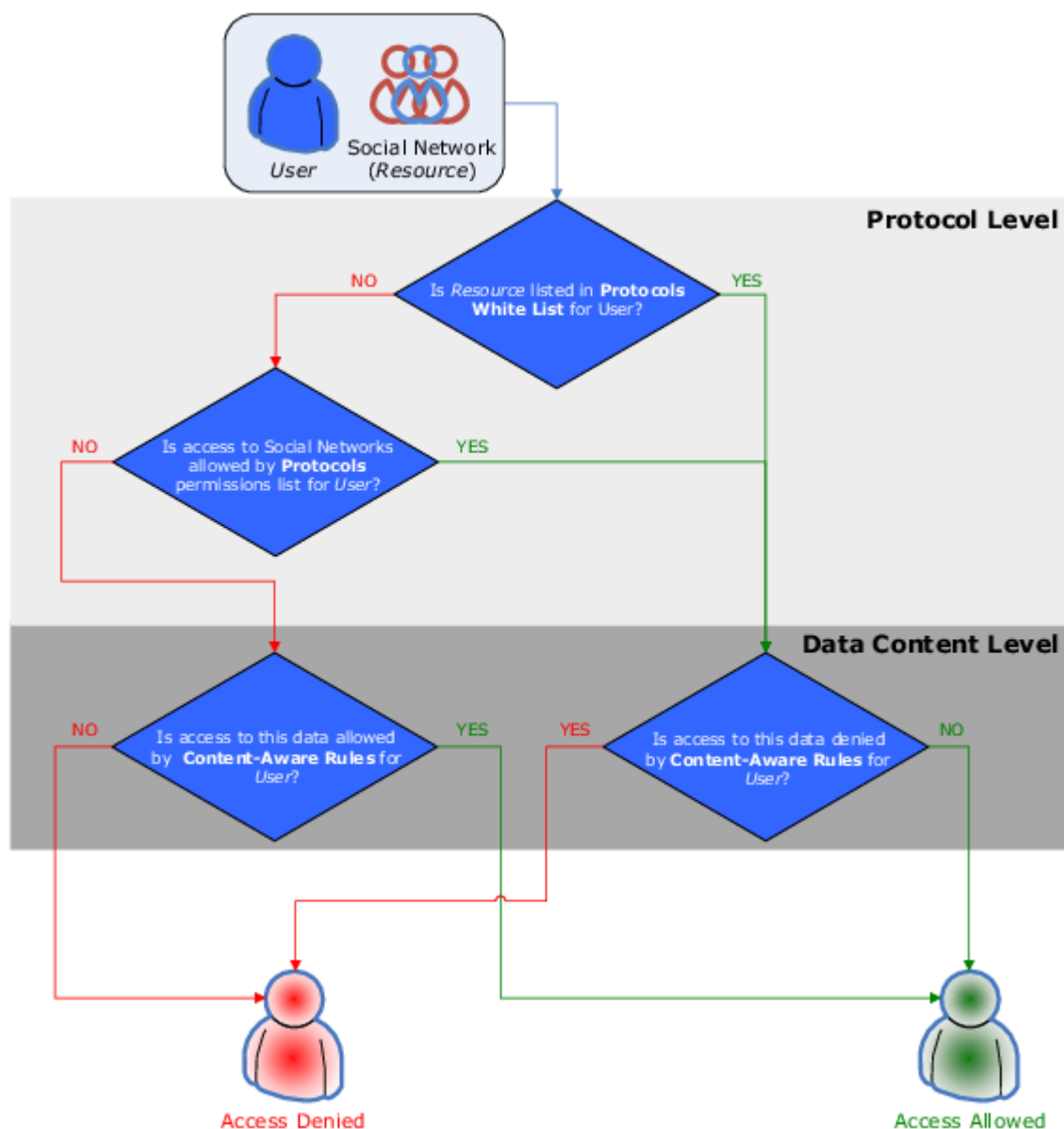
---

Access checking can occur at two levels: the protocol level and the data content level. All network connections are checked at both levels, except for connections using Telegram, Telnet, Torrent, and WhatsApp, which are checked at the protocol level only.

For example, suppose a user attempts to connect to a remote host. In this case, DeviceLock would first check whether the user is allowed the connection at the protocol level, and then it would check permissions at the data content level (Content-Aware Rules).



For another example, consider the case of a user connecting to a social networking site. Here DeviceLock would first check whether Social Networks are open or locked at the protocol level. Next, DeviceLock will also check permissions at the data content level (Content-Aware Rules).



Also, DeviceLock supports the white listing of protocols (see [Managing Protocols White List](#)). With the Protocols White List, you can turn off access control for connections with specific parameters (for example, HTTP connections to specific hosts and ports).

## DeviceLock Service for Mac

DeviceLock Service for Mac is designed to help network administrators prevent unauthorized data transfers, block file copying and prevent software uploads and downloads.

Supporting a wide range of storage protocols, media and devices, DeviceLock Service for Mac provides highly customizable and flexible access control to internal and external storage devices such CD, DVD, BD burners, external disks, floppy drives, USB drives and pen-drives; controls access to WiFi and Bluetooth adapters, and provides managed access to, USB, FireWire, and serial ports.



eSATA hardware can be controlled as Removable devices, while Thunderbolt devices can be controlled as Removable and WiFi hardware.

DeviceLock Service for Mac includes the following features:

- **Access Control for Ports and Storage Devices.** With DeviceLock Service for Mac, network administrators gain full control over who, when, and under what conditions can gain access to certain devices, ports. This helps prevent data leaks including unauthorized software installations.
- **Audits User Activities.** DeviceLock Service for Mac can audit user activity for a particular device type on a local computer. Based on the user's security context, this capability allows administrators to audit activities that belong to a certain user or user group. The tool can create log files collected by DeviceLock Enterprise Server and displayed by management consoles.
- **Data Shadowing.** DeviceLock Service for Mac enables administrators to see what information exactly has been transferred by creating a shadow copy of all data sent or received via certain ports or devices. The system uses data shadowing to mirror all data copied to external storage devices. A full copy of files being transferred can be saved to a SQL database. Data shadowing can be defined on per-user basis.
- **Active Directory Integration.** Tight integration into the Active Directory makes DeviceLock Service for Mac easier to configure and manage, simplifies permission management and maintenance in large heterogeneous networks. Integrating DeviceLock Service for Mac into a network domain allows retrieving configuration settings from Active Directory via DeviceLock Enterprise Server.

## DeviceLock Content Security Server

DeviceLock Content Security Server is an optional component of DeviceLock DLP. It includes Search Server which provides full-text searching of logged data stored on DeviceLock Enterprise Server, and Discovery Server used to discover certain types of content existing on the computers and storage devices connected to the local network. The search capabilities of Search Server make it easier and more efficient to manage the increasing amount of data in DeviceLock Enterprise Server databases.

Discovery Server, in its turn, is part of DeviceLock Discovery product, which can be used separately from-, or as a part of DeviceLock DLP. Discovery Server is described in the DeviceLock Discovery User Manual (see also [DeviceLock Discovery Overview](#)).

DeviceLock Content Security Server includes the following features:

- **Full-text search capability support.** Through the use of Search Server, DeviceLock Content Security Server allows you to instantly search for relevant text data based on various search criteria.
- **Ability to automate search operations.** DeviceLock Content Security Server can run searches by schedule, with search results being automatically sent via e-mail.
- **Flexible configuration options.** There is support for many different configuration options, enabling you to optimize the performance of DeviceLock Content Security Server for your unique installation.

You can use full-text searches to find data that you cannot find by filtering data in the log viewers. The full-text search functionality is especially useful in situations when you need to search for shadow copies of documents based on their contents.

You can operate DeviceLock Content Security Server by using the DeviceLock Management Console.

### ***Use Case - Preventing leaks of confidential information***

Security specialists who are tasked with keeping sensitive information confidential can regularly use Search Server to easily find, retrieve and analyze all shadow copies of files containing specific business-critical data, for example, customers or price lists. The log records associated with found shadow copies will help to determine when and by whom confidential information was copied. With this information, security specialists can take immediate steps to avoid possible information disclosure and distribution outside the company.

## How Search Server Works

Search Server performs the following functions:

- Indexes DeviceLock Enterprise Server data.
- Executes full-text queries after the data has been indexed.

These functions are described in more detail below.

## Indexing DeviceLock Enterprise Server Data

Indexing is a process through which the textual data on DeviceLock Enterprise Server becomes searchable and retrievable.

Search Server starts the indexing process automatically as soon as you specify DeviceLock Enterprise Server(s). The indexing process can result in either the creation or update of the full-text index. There is only one full-text index per Search Server, making management more efficient. The full-text index stores information about significant words and their location. During index creation or update, Search Server discards noise words (such as prepositions, articles, and so on) that do not help the search.

Search Server indexes all text data from the following sources: Audit Log, Shadow Log, Deleted Shadow Data Log, Server Log, Monitoring Log, and Policy Log.

The indexing process happens in two stages. In the first stage, Search Server extracts significant words from shadow copies and log records and saves them to temporary indexes for each specified DeviceLock Enterprise Server. For each temporary index, Search Server processes 1,000 records from each log. In the second stage, when either the number of temporary indexes becomes equal to 50 or 10 minutes pass, all temporary indexes are combined into a permanent master index that is used for search queries. The process of combining temporary indexes into a master index is called *merging*.

The creation of the master index is a time-intensive process. Indexing speed can vary considerably depending on the type of data being indexed and the hardware being used. Generally, indexing speed is between 30 and 120 MB/minute. Consider the following example:

- Data: 170 GB, consisting of 4,373,004 mixed-type files (HTML, office documents, text)
- Indexing time: 24.7 hours (6.8 GB/hour)
- Index size: 12% of original document size
- Hardware: Pentium® 4 Processor 550 (3.40GHz, 800 FSB), 2GB RAM, internal SATA RAID-0 drives

## Executing Search Queries

After the DeviceLock Enterprise Server data has been indexed, you can run full-text queries. These queries can search for one or more specific words or phrases. When a search query is executed, Search Server processes the query and retrieves a list of results from the index that matches the criteria of the query. Filtering can be applied to the search to narrow the result set returned. For example, the results can be filtered by log or date. Querying the full-text index is extremely fast and flexible. A search operation takes only seconds to locate and return matches for particular search criteria. For detailed information about the search results page and search results, see [Working with search results](#).

## ContentLock and NetworkLock

DeviceLock DLP comes with ContentLock and NetworkLock - separately licensed components that provide additional functionality for DeviceLock. These components are installed automatically but require a license to function. For more information on ContentLock and NetworkLock licenses, see [ContentLock and NetworkLock Licensing](#) later in this chapter.

---




### Note

ContentLock and NetworkLock are not yet supported in DeviceLock Service for Mac.

---

NetworkLock adds comprehensive context control capabilities over endpoint network communications. It supports port-independent network protocol and application detection and selective blocking, message and session reconstruction with file, data, and parameter extraction, as well as event logging and data shadowing. NetworkLock controls most popular network protocols and applications such as: plain and SSL-protected SMTP email communications (with messages and attachments controlled separately), communications between the Microsoft Outlook client and Microsoft Exchange Server (the MAPI protocol), IBM Notes, Web access and other HTTP-based applications including content inspection of encrypted HTTPS sessions (specifically, Web Mail, WhatsApp, and social networking applications like Gmail, Yahoo! Mail, Windows Live Mail, Facebook, Twitter, LiveJournal, etc.), instant messengers (Skype, Telegram, Viber, WhatsApp, ICQ Messenger, Jabber, IRC, Mail.ru Agent), cloud storages (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive, etc.), file transfers over FTP and FTP-SSL protocols, local network files transfers over SMB, as well as telnet and torrent sessions.

NetworkLock is represented in the user interface of DeviceLock Management Console, Service Settings Editor and DeviceLock Group Policy Manager by the **Protocols** node:

- >  Service Options
- >  Devices
- >  Protocols

NetworkLock has the following key features and benefits:

- **Protocol access control.** You can control which users or groups can gain access to the FTP, HTTP, IBM Notes, SMTP, MAPI (Microsoft Exchange), SMB, Telnet and Torrent protocols, instant messengers (Skype, Telegram, Viber, WhatsApp, ICQ Messenger, Jabber, IRC, Mail.ru Agent), cloud storages (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive, etc.), web search sites, career search web-sites, web-conferencing and webinars (Zoom.us), as well as webmail and social networking applications (ABV Mail, AOL Mail, freenet.de, Gmail, GMX Mail, Hotmail (Outlook.com), iCloud, Mail.ru, NAVER, Outlook Web App (OWA), Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail, Zimbra; Facebook, Google+, Instagram, LinkedIn, LiveJournal, Myspace, Odnoklassniki, Pinterest, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru) depending on the time of day and day of the week.
- **Protocols White List.** Lets you selectively allow network communication over specified protocols regardless of existing protocol blocking settings. The white list is most effective in “least privilege” scenarios when you block all protocol traffic and then specifically authorize only what is required for employees to perform their daily job duties.
- **Content-Aware Rules (File Type Detection).** You can selectively allow or deny access to specific types of files transmitted over the network. Recognition and identification of file types is based solely upon the content of files. This efficient and reliable algorithm allows for correct identification and handling of files regardless of the file extension. You can also use Content-Aware Rules to allow or deny the shadow copying of specific file types.

---

#### Note

A ContentLock license is required to gain access to enhanced capabilities of the Content-Aware Rules feature.

---

- **Audit, shadowing and alerts.** Provides the ability to track user activity for specified protocols, log a full copy of data/files transmitted over the network, and alert IS personnel to inappropriate user actions.

ContentLock is a content monitoring and filtering component that greatly enhances the capabilities of the Content-Aware Rules feature. With ContentLock, you can not only grant or deny access to information based on real file types but also create regular expressions patterns with numerical conditions and Boolean combinations of matching criteria and keywords. Recognizing more than eighty file formats and data types, ContentLock extracts and filters the content of data copied to removable drives and plug-n-play storage devices, as well as that transmitted over the network. With ContentLock, you can also filter shadowed data down to just those pieces of information meaningful to security auditing, incident investigations and forensic analysis before saving in the

Shadow Log. This tremendously reduces storage space and network bandwidth requirements for shadow log delivery to the central database.

ContentLock has the following key features and benefits:

- **Content-based document access control.** You can control access to documents depending on their content. Thus, you can block sensitive content leakage while allowing authorized employees to gain access to the information they need to collaborate.
- **Content-based filtering of shadow data.** You can specify that only data that contains sensitive information is shadow copied and saved to the Shadow Log, thus reducing the volume of unnecessary log data and making the log files easier to work with.
- **Content classification-based control of documents.** You can use digital fingerprints and Boldon James Classifier labels to control content access/sending permissions, content-aware shadowing, and/or simple content detection:
  - Digital fingerprints of sensitive documents are taken and stored on the DeviceLock Enterprise Server. Fingerprints can identify full copies as well as pieces of documents, even if the document has been changed.
  - In the Boldon James Classifier applications, classification labels specify the level of sensitivity of the document by appropriately setting its attributes.
- **Expansive coverage of multiple file formats and data types.** You can analyze content of the following file formats and data types: Adobe Acrobat (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128- or 256-bit AES, and the file permissions do not prevent text extraction) (\*.pdf), Adobe FrameMaker MIF (\*.mif), Ami Pro (\*.sam), Ansi Text (\*.txt), ASCII Text, ASF media files (metadata only) (\*.asf), AutoCAD (\*.dwg, \*.dxf), CSV (Comma-separated values) (\*.csv), DBF (\*.dbf), EBCDIC, EML (emails saved by Outlook Express) (\*.eml), Enhanced Metafile Format (\*.emf), Eudora MBX message files (\*.mbx), Flash (\*.swf), HTML (\*.htm, \*.html), iCalendar (\*.ics), Ichitaro (versions 5 and later) (\*.jtd, \*.jbw), JPEG (\*.jpg), Lotus 1-2-3 (\*.123, \*.wk?), MBOX email archives such as Thunderbird (\*.mbx), MHT archives (HTML archives saved by Internet Explorer) (\*.mht), MIME messages (including attachments), MSG (emails saved by Outlook) (\*.msg), Microsoft Access MDB files (\*.mdb, \*.accdb, including Access 2007 and Access 2010), Microsoft Document Imaging (\*.mdi), Microsoft Excel (\*.xls), Microsoft Excel 2003 XML (\*.xml), Microsoft Excel 2007, 2010, and 2013 (\*.xlsx), Microsoft OneNote 2007, 2010, and 2013 (\*.one), Microsoft Outlook data files (\*.PST), Microsoft Outlook/Exchange Messages, Notes, Contacts, Appointments, and Tasks, Microsoft Outlook Express 5 and 6 (\*.dbx) message stores, Microsoft PowerPoint (\*.ppt), Microsoft PowerPoint 2007, 2010, and 2013 (\*.pptx), Microsoft Rich Text Format (\*.rtf), Microsoft Searchable Tiff (\*.tiff), Microsoft Visio (\*.vsd, \*.vst, \*.vss, \*.vdw, \*.vsdx, \*.vssx, \*.vstx, \*.vsdm, \*.vssm, \*.vstm), Microsoft Word for DOS (\*.doc), Microsoft Word for Windows (\*.doc), Microsoft Word 2003 XML (\*.xml), Microsoft Word 2007, 2010, and 2013 (\*.docx), Microsoft Works (\*.wks), MP3 (metadata only) (\*.mp3), Multimate Advantage II (\*.dox), Multimate version 4 (\*.doc), OpenOffice versions 1, 2, and 3 documents, spreadsheets, and presentations (\*.sxc, \*.sxd, \*.sxi, \*.sxw, \*.sxd, \*.stc, \*.sti, \*.stw, \*.stm, \*.odt, \*.ott, \*.odg, \*.otg, \*.odp, \*.otp, \*.ods, \*.ots, \*.odf) (includes OASIS Open Document Format for Office Applications), Quattro Pro (\*.wb1, \*.wb2, \*.wb3, \*.qpw), QuickTime

(\*.\*mov, \*.\*m4a, \*.\*m4v), TIFF (metadata only) (\*.tif), TNEF (winmail.dat), Treepad HJT files (\*.hjt), Unicode (UCS16, Mac or Windows byte order, or UTF-8), Visio XML files (\*.vdx), Windows Metafile Format (\*.wmf), WMA media files (metadata only) (\*.wma), WMV video files (metadata only) (\*.wmv), WordPerfect 4.2 (\*.wpd, \*.wpf), WordPerfect (5.0 and later) (\*.wpd, \*.wpf), WordStar version 1, 2, 3 (\*.ws), WordStar versions 4, 5, 6 (\*.ws), WordStar 2000, Write (\*.wri), XBase (including FoxPro, dBase, and other XBase-compatible formats) (\*.dbf), XML (\*.xml), XML Paper Specification (\*.xps), XSL, XyWrite as well as PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, EMF spooled files and GDI printing (ZjStream).

---

#### Note

The content of AutoCAD (DWG, DXF) file formats can be analyzed on Windows XP and later systems.

---

- **Automated protection of new documents.** You can have content-based security policies automatically applied to new documents as they are created.
- **Multiple content detection methods.** Various methods can be used to identify sensitive content contained in documents (based on regular expressions, keywords, and document properties).
- **Centralized content management.** Content-Aware Rules are created based on content groups that enable you to centrally define the types of the content that is subject to control.
- **Ability to override device type/protocol-level policies.** You can selectively allow or deny access to certain content regardless of preset permissions at the device type-/protocol-level.
- **Inspection of files within archives.** Allows you to perform deep inspection of each individual file contained in an archive. The following inspection algorithm is used: When a user attempts to copy an archive file to a device or transmit it over the network, all files are extracted from the archive and analyzed separately to detect the content to which access is denied by Content-Aware Rules. If Content-Aware Rules deny access to at least one of the files extracted from the archive, the user is denied access to the archive. If Content-Aware Rules allow access to all of the files extracted from the archive, the user is allowed access to the archive.

---

#### Note

DeviceLock may skip inspecting fingerprints of files within an archive if it has detected an exact match of the archive file with a source file of a certain fingerprint. For details, see [Inspecting fingerprints within archives](#) in the [Digital Fingerprints](#) section of this document.

---

All archived files are extracted to the Temp folder of the System user. Typically, the system Temp folder resides in the following location: %windir%\Temp. If DeviceLock Service cannot access the Temp folder, the archived files are not analyzed and access to the archive is denied only if any one of the following conditions is true:

- There is a Deny Content-Aware Rule
- Deny-access permissions are set for the device type or protocol

All nested archives are also unpacked and analyzed one by one. Archive files are detected by content, not by extension. The following archive formats are supported: 7z (.7z), ZIP (.zip), GZIP

(.gz, .gzip, .tgz), BZIP2 (.bz2, .bzip2, .tbz2, .tbz), TAR (.tar), RAR (.rar), CAB (.cab), ARJ (.arj), Z (.z, .taz), CPIO (.cpio), RPM (.rpm), DEB (.deb), LZH (.lzh, .lha), CHM (.chm, .chw, .hxs), ISO (.iso), UDF (.iso), COMPOUND (.msi), WIM (.wim, .swm), DMG (.dmg), XAR (.xar), HFS (.hfs), NSIS (.exe), XZ (.xz), MSLZ (.mslz), VHD (.vhd), FLV (.flv), SWF (.swf) as well as CramFS, SquashFS (.squashfs), NTFS, FAT, and MBR file system and disk images. Split (or multi-volume) and password-protected archives are not unpacked.

---

## Note

To allow transfer of split (multi-volume) archives in case of content-aware rules combined with [Archives content inspection on read](#) or [Archives content inspection on write](#) option enabled in [Service Options](#), configure allow rules based on [Document Properties Content Groups](#) with the **Text extraction not supported** flag selected.

---

- **Optical Character Recognition (OCR).** The use of the OCR technology allows you to recognize and extract text from scanned documents, camera-captured documents (if these documents were aligned 90 degrees to the camera), and screen shots of documents for further content analysis by Content-Aware Rules.

OCR includes the following capabilities:

- An entire image or some portions of the image can be inverted, rotated, or mirrored.
- Images with poor brightness or low contrast are supported.
- Most fonts can be accurately recognized.

OCR includes the following limitations:

- Recognition of handwritten text or any fonts that look like handwritten text is not supported.
- Embossed and engraved texts are not recognized.
- Best recognition results are achieved for black text on a white background.

The built-in OCR supports the following languages: Arabic, Bulgarian, Catalan, Chinese - Simplified, Chinese - Traditional, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, and Turkish. The following image files are supported for OCR processing: BMP files, Dr. Halo CUT files, DDS files, EXR files, Raw Fax G3 files, GIF files, HDR files, ICO files, IFF files (except Maya IFF files), JBIG files, JNG files, JPEG/JIF files, JPEG-2000 files, JPEG-2000 codestream files, KOALA files, Kodak PhotoCD files, MNG files, PCX files, PBM/PGM/PPM files, PFM files, PNG files, Macintosh PICT files, Photoshop PSD files, RAW camera files, Sun RAS files, SGI files, TARGA files, TIFF files, WBMP files, XBM files, and XPM files.

---

## Note

The OCR feature is only supported on Windows XP and later versions of Windows.

---

- **Text in picture detection.** The use of the text in picture detection technology allows you to classify all images into two groups: text images (containing text, such as scanned documents or screen shots of documents) and non-text images (those that do not contain text), and separately control access to each group. For example, you can allow certain users to copy non-text images to



devices, but prevent them from writing text images thus preventing leakage of sensitive information within image files. The following image files are supported: BMP files, Dr. Halo CUT files, DDS files, EXR files, Raw Fax G3 files, GIF files, HDR files, ICO files, IFF files (except Maya IFF files), JBIG files, JNG files, JPEG/JIF files, JPEG-2000 files, JPEG-2000 codestream files, KOALA files, Kodak PhotoCD files, MNG files, PCX files, PBM/ PGM/PPM files, PFM files, PNG files, Macintosh PICT files, Photoshop PSD files, RAW camera files, Sun RAS files, SGI files, TARGA files, TIFF files, WBMP files, XBM files, and XPM files.

- **Inspection of images embedded in documents.** Allows you to perform deep inspection of each individual image embedded in saved emails (EML), Adobe Portable Document Format (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx). All embedded images are extracted from these documents to the Temp folder of the System user and analyzed independently from text to detect the content to which access is denied by Content-Aware Rules. The text contained inside documents is checked by Content-Aware Rules that are created based on Keywords, Pattern or Complex content groups. Embedded images are checked by Content-Aware Rules that are created based on Keywords, Pattern, File Type Detection, Document Properties or Complex content groups. Access to documents is granted only when Content-Aware Rules allow access to text and all of the images contained in documents.

---

#### Note

Deep inspection of images embedded in files of AutoCAD (DWG, DXF) formats can be performed on Windows XP and later systems only.

---

## ContentLock and NetworkLock Licensing

If you want to use NetworkLock and/or ContentLock, you must purchase NetworkLock and/or ContentLock licenses in addition to the Core DeviceLock license.

A NetworkLock license enables you to use the Protocols feature.

A ContentLock license enables you to create and use Content-Aware Rules based on regular expressions, keywords, and document properties as well as complex rules based on Boolean combinations of matching criteria.

If you use different types of licenses, consider the following:

- If you have a Core DeviceLock license, ContentLock license, and NetworkLock license, you can use the Protocols feature, create and use Content-Aware Rules based on file types, regular expressions, keywords, and document properties as well as complex rules.
- If you have only a Core DeviceLock license, you cannot use the Protocols feature, and you cannot create and use Content-Aware Rules based on regular expressions, keywords, and document properties as well as complex rules. You can create and use Content-Aware Rules based on file types (File Type Detection).



- If you have a Core DeviceLock license and ContentLock license, you can create and use Content-Aware Rules based on file types, regular expressions, keywords, and document properties as well as complex rules. You cannot use the Protocols feature.
- If you have a Core DeviceLock license and NetworkLock license, you can use the Protocols feature and create and use Content-Aware Rules based on file types. You cannot create and use Content-Aware Rules based on regular expressions, keywords, and document properties as well as complex rules.
- A Core DeviceLock license is mandatory, while NetworkLock and ContentLock licenses are optional. If a Core license is missing or invalid, DeviceLock runs in a trial mode only. The number of NetworkLock and/or ContentLock licenses must be equal to the number of Core DeviceLock licenses.
- The trial period for ContentLock and NetworkLock is 30 days.

## User Activity Monitor (UAM)

DeviceLock DLP includes User Activity Monitor (UAM) - an optional component that extends the functionality of DeviceLock. It installs automatically but requires a separate license to function. For more information on a license for this component, see [UAM Licensing](#).

The DeviceLock UAM component provides the ability to monitor end user actions by video recording of the user's computer screen, as well as recording all keystrokes and information about the processes and applications that were running and used during recording. These kinds of activity monitoring significantly expand the evidence base in the investigation of information security incidents, simplify the process of identifying suspicious user behavior, and help reveal misuse of access privileges or data protection policies, thereby reducing risks of data leaks.

An important feature of DeviceLock UAM is the ability to record a computer screen, keystrokes, and process information when a specific event occurs. DeviceLock UAM rules can be set to start recording upon various event occurrences, such as triggering a certain content inspection rule, connecting an external drive, running a certain process in the system, etc.

To implement user activity monitoring, DeviceLock Service records the user's on-screen actions in a video format along with recording user keystrokes and saving other information such as active application name, active window title, and so on. The monitoring data can then be collected from user computers by DeviceLock Enterprise Server where authorized persons can view and analyze those recordings of user activity.

The ability to store a recording of user actions gives DeviceLock a number of advantages when detecting data leak threats. The DeviceLock Service records exactly what the user sees on the computer screen regardless of applications and protocols used or level of privilege the user has. Keyboard input and other data recorded by DeviceLock Service along with video can be leveraged to track certain user actions.

DeviceLock Service features various triggering criteria to start recording when certain events or conditions occur. Depending on the criteria selected in the policy, recording can start, for example, when a specific device is connected, a certain application is opened, or an unauthorized attempt is

made to write a file or send a message. Triggering criteria enable DeviceLock Service to perform selective recordings of potentially suspicious user actions. Here are some example of the triggering criteria available:

- VPN connection exists
- Wireless connection exists
- Process "<process name>" exists
- Content-Aware rule "<rule name>" is triggered
- Storage device is attached
- Read access to "<device / protocol name>" is denied
- Write access to "<device / protocol name>" is denied

For more on record triggering criteria, see [Setting up triggering criteria](#) in the [User Activity Monitor](#) documentation.

DeviceLock Service initially stores user activity monitoring data on the local computer, allowing the administrator to explore local records of user actions in the DeviceLock Management Console connected to the DeviceLock Service. In this way, one can only view the records made by the DeviceLock Service on the local computer.

To enable a centralized viewing and analysis of the recordings made on different computers, it is necessary to transfer user activity monitoring data to DeviceLock Enterprise Server. The servers to collect and hold that data are specified by the respective DeviceLock Service setting. If necessary, the data from individual servers can be combined for viewing and analysis on a central collection server by using the log consolidation feature.

For more on monitoring record viewers, see [Viewing User Activity](#) in the [User Activity Monitor](#) documentation.

## UAM Licensing

To enable User Activity Monitor, the DeviceLock UAM volume license must be acquired and installed in addition to the DeviceLock Core license. The UAM license determines the maximum permitted number of computers that have DeviceLock Service employed to monitor user activity.

Install the UAM license on the computer running the DeviceLock Management Console to administer User Activity Monitor on computers with the DeviceLock Service:

- View or change UAM options.
- Set up, view, or change UAM recording rules.
- View UAM records on the DeviceLock Service.

To apply server policies and computer monitoring tasks that include UAM options and rules, the DeviceLock Enterprise Server must have the UAM license installed. The number of computers to which such policies and tasks are applied cannot be more than the UAM license specifies.

To collect UAM data, the DeviceLock Enterprise Server must have the Core license installed. The number of computers from which the server collects UAM data cannot be more than the Core license specifies.

When planning for the UAM license, consider the following:

- User Activity Monitor cannot be used without the DeviceLock Core license. The Core license must be installed on the computer running the DeviceLock Management Console. Otherwise, DeviceLock runs in trial mode for 30 days only.
- The number of computers specified in the UAM license must be equal to the number of computers specified in the Core license. Otherwise, UAM runs in trial mode for 30 days only.
- The UAM license is optional, and affects only the UAM component. Other DeviceLock features and components, if properly licensed, are available regardless of whether a UAM license is installed.

## Basic Security Rules

Following is a series of basic security rules that should be met for computers that you want to install in a corporate network:

- **Change the boot sequence.** The hard disk must be the first boot device. Change the boot sequence in the BIOS so that the computer does not boot from the floppy, USB drive or CD-ROM. If the hard disk is not the first boot device, someone can use a bootable CD or USB Flash Drive to directly access the hard disk drive.
- **Protect the BIOS with a password.** The password should be set to the BIOS so only an authorized person can make changes there. If the BIOS is not password protected, someone can change the boot sequence and use a bootable CD, floppy or USB Flash Drive (see above).
- **Seal computer cases and chassis.** Protect the hardware with a seal. Otherwise, it is possible to plug an external boot device directly to the computer and access the hard disk. Moreover, if someone can physically access the motherboard, it is very easy to locate the CMOS reset jumper and clear the BIOS password (see above).
- **Do not give administrator rights to regular users.** Regular local users should not be members of the local Administrators group. It is not a good practice to grant users administrative rights to their computers.  
*However, if for some reason users on your network have administrator privileges on their local computers, DeviceLock provides another level of protection. No one except authorized DeviceLock administrators can connect to, stop, or uninstall DeviceLock Service. Even members of the local Administrators group cannot disable DeviceLock if they are not in the list of the authorized DeviceLock administrators.*
- **Remove the Windows Recovery Environment/Recovery Console.** By using Windows Recovery Environment on a local computer, anyone can restart the computer in recovery mode and work around all security measures, including disabling DeviceLock Service (however, this requires the local administrator password). For this reason, we recommend preventing the use of Windows Recovery Environment by regular users. System recovery options are described in Microsoft's

article at [support.microsoft.com/en-us/kb/307654](https://support.microsoft.com/en-us/kb/307654). For information about Windows Recovery Environment, see Microsoft's article at [msdn.microsoft.com/en-us/dn938364](https://msdn.microsoft.com/en-us/dn938364).

# Installing DeviceLock

## System Requirements

DeviceLock DLP includes DeviceLock Service, DeviceLock Enterprise Server, DeviceLock Content Security Server, and management consoles: DeviceLock Management Console, DeviceLock Group Policy Manager, and DeviceLock Enterprise Manager. This section covers system requirements for each of these components.

The computer to run DeviceLock Service must meet the following requirements:

<b>Operating system for DeviceLock Service for Windows</b>	Microsoft Windows 7/8/8.1/10/11, Windows Server 2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022  Installation is supported on both 32-bit and 64-bit operating systems.
<b>Operating system for DeviceLock Service for Mac</b>	macOS 10.15 (Catalina), macOS 11.2.3 (Big Sur) or macOS 12 (Monterey)
<b>Memory (RAM)</b>	Minimum: 1024 MB
<b>Hard disk space</b>	Minimum: 400 MB
<b>Processor</b>	Minimum: Intel Pentium 4
<b>Supported virtualization platforms</b>	Microsoft Remote Desktop Services, Citrix XenDesktop / XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox, and Windows Virtual PC.

---

### Note

DeviceLock Service can only record user activity on computers running Windows 7 / Windows Server 2008 R2 or later.

---

The computer to run DeviceLock management consoles must meet the following requirements:

<b>Operating system</b>	Microsoft Windows 7/8/8.1/10/11, Windows Server 2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022  Installation is supported on both 32-bit and 64-bit operating systems.
<b>Memory (RAM)</b>	Minimum: 1024 MB
<b>Hard disk space</b>	Minimum: 1 GB
<b>Processor</b>	Minimum: Intel Pentium 4

---

**Note**

- Internet Explorer 9 or later is required to view Relations Charts, operate Search Server, administer Digital Fingerprints, work with the UAM Log, and view reports in Discovery Server.
  - Internet Explorer 11 or later is required to view User Dossiers.
  - To view UAM Log records, the console must be installed on a computer running Windows 7 / Windows Server 2008 R2 or later.
    - To view UAM Log videos in the console on Windows Server, the Desktop Experience / Media Foundation feature must be installed.
    - To view UAM Log videos in the console on Windows N or KN, the Media Feature Pack must be installed. For installation instructions, see [support.microsoft.com/help/3145500](https://support.microsoft.com/help/3145500).
- 

The DeviceLock Enterprise Server system requirements are as follows:

<b>Operating system</b>	Microsoft Windows 7/8/8.1/10/11, Windows Server 2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022  Installation is supported on both 32-bit and 64-bit operating systems.
<b>Memory (RAM)</b>	Minimum: 1 GB  Recommended: 8 GB
<b>Hard disk space</b>	Minimum: 1 GB  Recommended: 800 GB (in case of local database server)
<b>Processor</b>	Minimum: Intel Pentium 4  Recommended: 2x Intel Xeon Quad Core 2.33 GHz
<b>Database server</b>	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017, 2019, or 2022 any edition, including SQL Server Express  - OR -  PostgreSQL 9.5 (9.5.19 or later), 9.6 (9.6.15 or later), 10 (10.10 or later), 11 (11.5 or later), or 12 (12.0 or later).  PostgreSQL ODBC Driver version 9.6.500 or later. The latest driver version is preferred.

---

**Important**

With PostgreSQL as the database server, the DeviceLock Enterprise Server provides for collecting and administering Audit Log, Shadow Log, Deleted Shadow Data Log, and Server Log, including the [consolidation](#) of these Logs. Other features of DeviceLock Enterprise Server in this case are not available.

---

The DeviceLock Content Security Server system requirements are as follows:

<b>Operating system</b>	Microsoft Windows 7/8/8.1/10/11, Windows Server 2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022  Installation is supported on both 32-bit and 64-bit operating systems.
<b>Memory (RAM)</b>	Minimum: 1 GB Recommended: 8 GB
<b>Hard disk space</b>	Minimum: 1 GB Recommended: 800 GB (in case of local database server)
<b>Processor</b>	Minimum: Intel Pentium 4  Recommended: 2x Intel Xeon Quad Core 2.33 GHz
<b>Database server</b>	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017, 2019, or 2022 any edition, including SQL Server Express

To install and configure DeviceLock, you need administrator rights. To install and configure DeviceLock only on a standalone computer, you must be a local administrator. To install and configure DeviceLock on computers in an Active Directory domain, you must be a domain admin.

To use DeviceLock on the network, a functioning TCP/IP network protocol is required. However, DeviceLock can also work on standalone computers. A network is needed only if you want to control DeviceLock Service from a remote computer.

Open the following TCP/UDP ports to enable network communication and data exchange among DeviceLock components:

- 135 (TCP) - RPC (Remote Procedure Call) endpoint mapper port.
- 137 (UDP) - NetBIOS Name Resolution port.
- 138 (UDP) - NetBIOS Datagram Service port.
- 139 (TCP) - NetBIOS Session Service port.
- 445 (TCP) - Server Message Block (SMB) port. Used by the DeviceLock Management Console when managing the DeviceLock Service on remote computers.
- 9132 (TCP) - DeviceLock Service's default port.
- 9133 (TCP) - DeviceLock Enterprise Server's default port. This port is also used by default for [log consolidation](#), and should be open on both the remote and central collection servers.
- 9134 (TCP) - DeviceLock Content Security Server's default port.

Additionally, set the startup type of "Automatic" for the following services:

- Remote Registry
- Remote Procedure Call (RPC)
- Base Filtering Engine

---

**Note**

Setting the startup type of the Base Filtering Engine service is required only on Windows 8 or later.

---

***Additional system requirements for Discovery Agents***

DeviceLock Discovery Server, an integral part of DeviceLock Content Security Server, can deploy and manage DeviceLock Discovery Agents on client computers. The following requirements apply to Discovery Agent installations:

<b>Operating system</b>	Microsoft Windows 7/8/8.1/10/11, Windows Server 2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022  Installation is supported on both 32-bit and 64-bit operating systems.
<b>Memory (RAM)</b>	Minimum: 1024 MB
<b>Hard disk space</b>	Minimum: 200 MB
<b>Processor</b>	Minimum: Intel Pentium 4

Open the following TCP/UDP ports to enable the Discovery Agent to communicate over the network with other DeviceLock components, and to scan SMB resources:

- 135 (TCP) - RPC (Remote Procedure Call) endpoint mapper port.
- 137 (UDP) - NetBIOS Name Resolution port.
- 138 (UDP) - NetBIOS Datagram Service port.
- 139 (TCP) - NetBIOS Session Service port.
- 9135 (TCP) - Discovery Agent's default port.
- 445 (TCP) - Server Message Block (SMB) port. Used when scanning SMB resources on remote computers.

## Deploying DeviceLock Service for Windows

DeviceLock Service should be installed on the computer so you can control the access to devices and network protocols on that computer. There are several ways to deploy DeviceLock Service to client systems:

- [Interactive Installation](#)
- [Unattended Installation](#)
- [Installation via Microsoft Systems Management Server](#)
- [Installation via DeviceLock Management Console](#)
- [Installation via DeviceLock Enterprise Manager](#)
- [Installation via Group Policy](#)
- [Installation via DeviceLock Enterprise Server](#)

***Recommendations***



Due to the specifics of DeviceLock Service operation, antiviruses can mistake DeviceLock executable files for malware and perform unscheduled scanning of its service folders. This can cause a noticeable decrease in the performance of DeviceLock Service and the computer itself, as well as lead to other problems.

To prevent loss of performance on a computer with DeviceLock Service installed, it is advisable to add the following folders to the list of exclusions for antivirus:

1. DeviceLock installation folder - By default, this is %ProgramFiles%\DeviceLock or %ProgramFiles (x86)%\DeviceLock on a 32-bit or 64-bit system, respectively.
2. DeviceLock shadowing folder - By default, this is %SystemRoot%\SHADOW, and can be changed by the [Local storage directory](#) option setting.

## Interactive Installation

Run Setup (setup.exe) and follow the instructions on the wizard pages that appear on the screen.

---

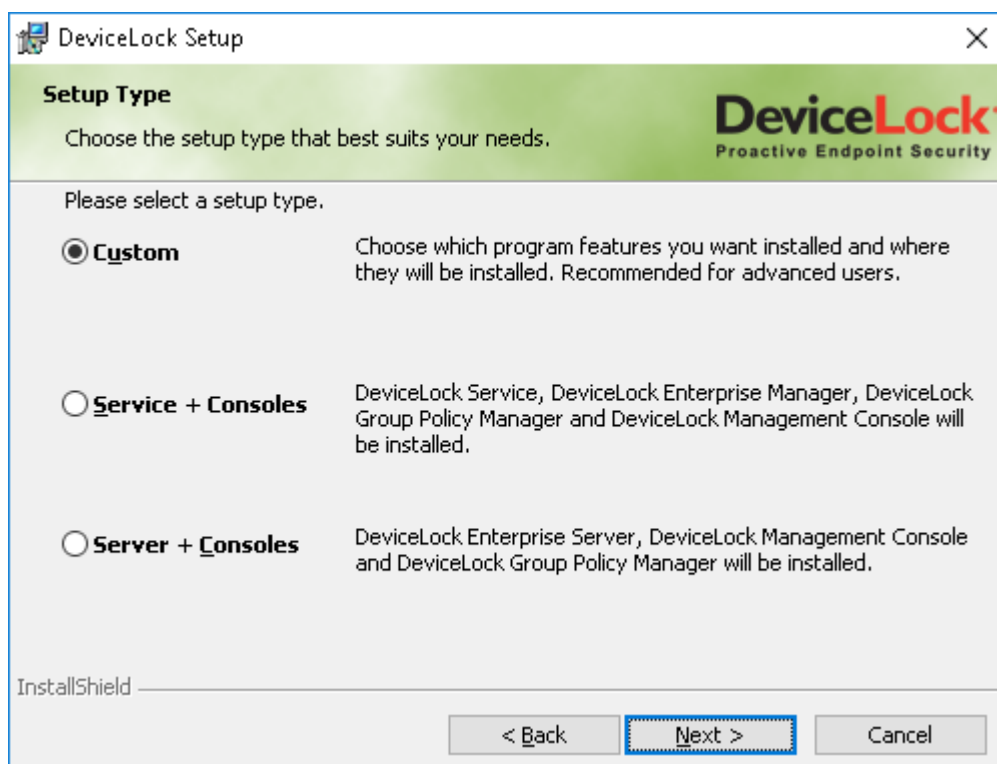
### Note

- You should run setup.exe on each computer that is to be controlled with DeviceLock Service.
  - If you are upgrading a previous version, make sure that you have administrative access to DeviceLock Service, otherwise you will not be able to continue installation.
- 

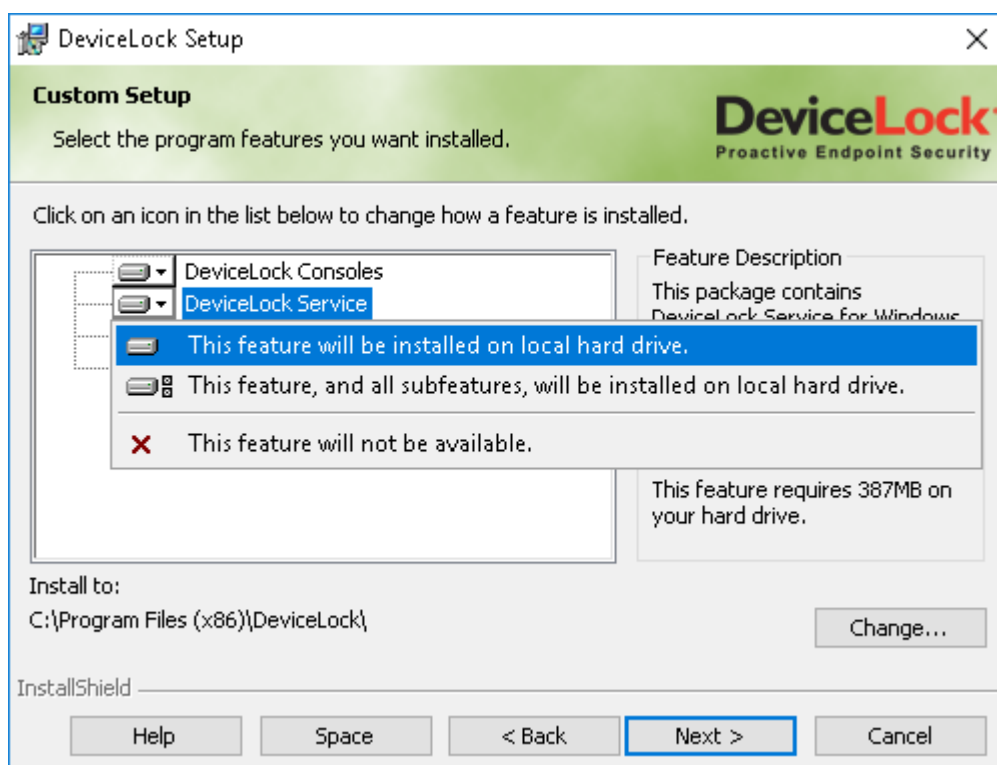
On the **License Agreement** page, read the License Agreement and then click **I accept the terms in the license agreement** to accept the licensing terms and conditions and proceed with the installation.

On the **Customer Information** page, type your user name and organization.

On the **Setup Type** page, select the required setup type.



You have the following two choices: either install both DeviceLock Service and DeviceLock management consoles using the **Service + Consoles** option or install only DeviceLock Service using the **Custom** option and selecting the **DeviceLock Service** component.



---

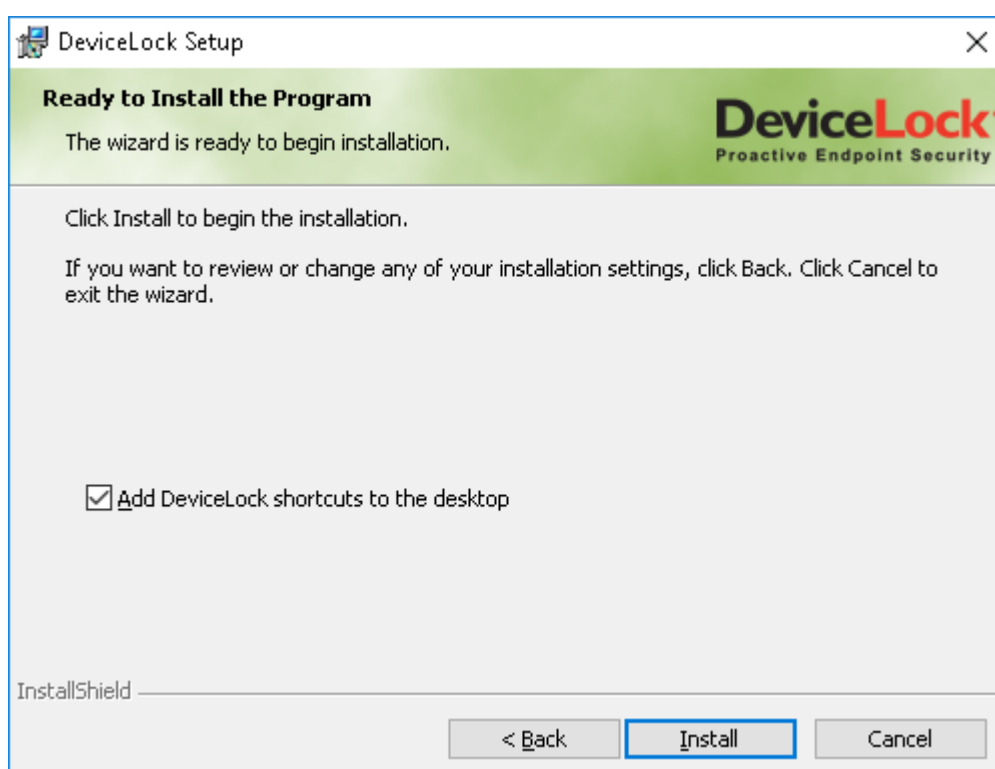
**Note**

On the **Custom Setup** page, you can select the RSoP component to install. This component enables support for DeviceLock's Resultant Set of Policy planning mode on domain controllers. The RSoP component is required only when DeviceLock management consoles are installed, but DeviceLock Service is not installed on the computer. For more information on RSoP planning mode, refer to Microsoft's documentation at [technet.microsoft.com/library/cc758010.aspx](https://technet.microsoft.com/library/cc758010.aspx).

---

On the **Custom Setup** page, you can change the default installation folder. Click **Change** and then choose a folder in the dialog box that appears. The default folder is %ProgramFiles%\DeviceLock.

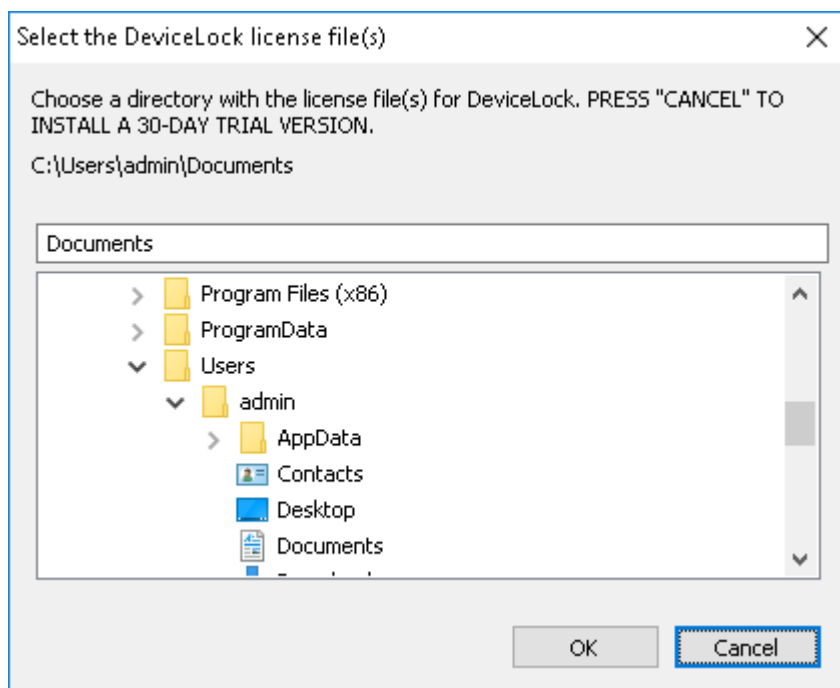
On the **Ready to Install the Program** page, click **Install** to begin the installation. Select the **Add DeviceLock shortcuts to the desktop** check box to add DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Service Settings Editor shortcuts to the desktop.



If you choose to install DeviceLock management consoles as well, Setup may suggest that you generate a new DeviceLock Certificate. The following message will appear: "Do you want to create the new DeviceLock Certificate (the private and public key pair)? Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair."

You can always generate a new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just click the **No** button and continue the installation. For more information on DeviceLock Certificates, see the [DeviceLock Certificates](#) section later in this document.

Also, if you select **Service + Consoles**, Setup may suggest that you load the DeviceLock license files. If you don't have the license files, click **Cancel** to install DeviceLock in a 30-day trial mode.



For further information about DeviceLock licenses, see [Activating Client Licenses](#).

During the installation process, you can set special permissions for local devices and protocols.

Lock Channels

Lock automatically:

<input type="checkbox"/> BlackBerry	<input checked="" type="checkbox"/> Floppy Drives	<input type="checkbox"/> Parallel Ports	<input type="checkbox"/> TS Devices
<input type="checkbox"/> Bluetooth Adapters	<input type="checkbox"/> Infrared Ports	<input type="checkbox"/> Printers	<input type="checkbox"/> USB Ports
<input type="checkbox"/> Clipboard	<input type="checkbox"/> iPhone	<input checked="" type="checkbox"/> Removable Devices	<input type="checkbox"/> WiFi (802.11) Adapters
<input checked="" type="checkbox"/> Optical Drives	<input type="checkbox"/> MTP	<input type="checkbox"/> Serial Ports	<input type="checkbox"/> Windows Mobile Devices
<input type="checkbox"/> FireWire Ports (IEEE 1394)	<input type="checkbox"/> Palm Devices	<input type="checkbox"/> Tape Devices	

---

<input type="checkbox"/> Career Search	<input type="checkbox"/> Jabber	<input type="checkbox"/> SMTP	<input type="checkbox"/> Web Mail
<input type="checkbox"/> File Sharing	<input type="checkbox"/> Mail.Ru Agent	<input type="checkbox"/> Social Networks	<input type="checkbox"/> Web Search
<input type="checkbox"/> FTP	<input type="checkbox"/> MAPI	<input type="checkbox"/> Telegram	<input type="checkbox"/> WhatsApp
<input type="checkbox"/> HTTP	<input type="checkbox"/> IBM Notes	<input type="checkbox"/> Telnet	<input type="checkbox"/> Zoom
<input type="checkbox"/> ICQ Messenger	<input type="checkbox"/> Skype	<input type="checkbox"/> Torrent	
<input type="checkbox"/> IRC	<input type="checkbox"/> SMB	<input type="checkbox"/> Viber	


☒ Create local groups (Allow\_Access\_to\_...) if not existing

Security Settings:

<input type="checkbox"/> Access control for USB HID (mouse, keyboard, etc.)
<input checked="" type="checkbox"/> Access control for USB printers
<input checked="" type="checkbox"/> Access control for USB scanners and still image devices
<input type="checkbox"/> Access control for USB Bluetooth adapters
<input checked="" type="checkbox"/> Access control for USB storage devices
<input checked="" type="checkbox"/> Access control for USB audio devices
<input checked="" type="checkbox"/> Access control for USB cameras
<input checked="" type="checkbox"/> Access control for USB and FireWire network cards
<input checked="" type="checkbox"/> Access control for FireWire storage devices
<input checked="" type="checkbox"/> Access control for serial modems (internal and external)
<input checked="" type="checkbox"/> Access control for virtual Optical Drives (Windows 2000 and later)
<input type="checkbox"/> Access control for virtual printers (Windows 2000 and later)
<input checked="" type="checkbox"/> Access control for intra-application copy/paste clipboard operations
<input type="checkbox"/> Block FireWire controller if access is denied
<input type="checkbox"/> Treat TS forwarded USB devices as regular ones
<input checked="" type="checkbox"/> Switch PostScript printer to non-PostScript mode
<input checked="" type="checkbox"/> Access control for Bluetooth HID (mouse, keyboard, etc.)

---

<input type="checkbox"/> Block unrecognized outgoing SSL traffic	<input checked="" type="checkbox"/> Intercept MS Lync connections
<input type="checkbox"/> Block IP addresses in URL	<input checked="" type="checkbox"/> Intercept draft MAPI messages
<input type="checkbox"/> Block proxy traffic	<input checked="" type="checkbox"/> Intercept moved MAPI messages
<input checked="" type="checkbox"/> Block Tor Browser traffic	
<input checked="" type="checkbox"/> Block network if BFE service is stopped (Windows 8 and later)	

 If you intend to manage DeviceLock policy settings on networks with either group/server policy or traditional DeviceLock consoles from a central location, please skip this step.

OK Skip

Select devices and/or protocols you would like to set permissions to. Select the **Create local groups (Allow\_Access\_to\_...) if not existing** check box for Setup to create the special local user group Allow\_Access\_To\_ for each channel type (e.g. Allow\_Access\_To\_Floppy for floppy drives), if these do not exist on the local computer.

Setup assigns **Read, Write, Format** and **Eject** generic rights to members of the Administrators group and the SYSTEM account. Members of the Allow\_Access\_To\_ group will have **Read, Write** and **Eject** generic rights.

Also, you can define security settings to exclude certain types of devices from the access check (see [Security Settings \(Regular Profile\)](#)).

Select **Access control for USB HID**, **Access control for USB printers**, **Access control for USB scanners and still image devices**, **Access control for USB Bluetooth adapters**, **Access control for USB storage devices** or **Access control for FireWire storage devices** to allow DeviceLock Service to control security for Human Interface Devices (mouse, keyboard, etc.), printers, scanners and still image devices, Bluetooth adapters or storage devices (such as flash drives) plugged into the USB and FireWire port. To allow access control for Web cameras and/or audio devices plugged into the USB port, check **Access control for USB cameras** and/or **Access control for USB audio devices**. To allow access control for USB and FireWire network cards, check **Access control for USB and FireWire network cards**. Otherwise, even if the USB and/or FireWire ports are locked, the devices listed above will continue to function as usual when connected to those ports. To allow access control for serial modems (internal and/or external), select **Access control for serial modems**. To disable locking of virtual (software emulated) CD/DVD/BD, uncheck **Access control for virtual Optical Drives**. To disable control of virtual printers (those which print to files), uncheck **Access control for virtual printers**. To allow access control for copy/paste clipboard operations within an application, select the **Access control for intra-application copy/paste clipboard operations** check box. Otherwise, even if the clipboard is locked, access control for copy/paste operations within one application is disabled. To disable FireWire controllers when the Everyone account has No Access permissions for the FireWire port device type, select the **Block FireWire controller if access is denied** check box. To allow access control for Bluetooth Human Interface Devices (mouse, keyboard, etc.), select **Access control for Bluetooth HID (mouse, keyboard, etc.)**.

Select the **Switch PostScript printer to non-PostScript mode** check box to make PostScript printers act like non-PostScript printers. This resolves an issue in which DeviceLock Service is unable to create a correct shadow copy of printed data and perform content analysis of data sent to printers that use a PostScript driver.

Select the **Treat TS forwarded USB devices as regular ones** check box to allow DeviceLock Service to control access to all USB devices redirected during a Citrix XenDesktop/MS RemoteFX session according to the rights set for the USB port device type. Otherwise, DeviceLock Service controls access to all USB devices redirected during a Citrix XenDesktop/MS RemoteFX session according to the **USB Devices Access** right set for TS Devices.

Also, you can define security settings for protocols (see [Managing Security Settings for Protocols](#)).

To allow DeviceLock Service to audit and block all unrecognized outgoing SSL traffic, select the **Block unrecognized outgoing SSL traffic** check box. Otherwise, even if the protocols are locked, all unrecognized outgoing SSL traffic is not blocked and audit is not performed for it.

To allow DeviceLock Service to block all URLs containing the host IP address when users have “allow access” permissions for the HTTP protocol, select the **Block IP addresses in URL** check box. This setting blocks, for instance, access to Web-sites by IP address.

To allow DeviceLock Service to audit and block all traffic that flows through a proxy server, select the **Block proxy traffic** check box. The following proxy servers are supported: HTTP, SOCKS4, and SOCKS5.

To allow DeviceLock Service to block connection to the Tor network, preventing the use of the Tor Browser, select the **Block Tor Browser traffic** check box.

To force DeviceLock Service to block all network traffic when the Base Filtering Engine system service is stopped, select the **Block network if BFE service is stopped (Windows 8 and later)** check box.

To allow DeviceLock Service to intercept network traffic from Microsoft Lync 2010 or Microsoft Office Communicator, select the **Intercept MS Lync connections** check box.

To allow DeviceLock Service to control draft folder messages that Outlook saves to the Exchange Server, select the **Intercept draft MAPI messages** check box.

To allow DeviceLock Service to control messages that Outlook imports to the Exchange Server from e-mail message export files (.msg files) or other (external) mailboxes, select the **Intercept moved MAPI messages** check box.

Click **OK** to apply changes. Click **Skip** if you prefer to wait until after installation to set permissions to these devices using DeviceLock management consoles.

Then, on the **Installation Wizard Completed** page, click **Finish** to complete the installation. On this page, there is the option to go to the DeviceLock home page. This option is selected by default.

---

## Note

You can uninstall DeviceLock as follows:

- Use **Programs and Features** in Control Panel (**Add or Remove Programs** on earlier versions of Windows) to remove **DeviceLock**.  
- OR -
  - Select **Remove DeviceLock** on the Windows **Start** menu.
- 

## Unattended Installation

DeviceLock also supports unattended (silent) installation. This provides an installation method that can be used from within a batch file. To install DeviceLock Service without user interaction, run the file `setup.exe` with the `/s` parameter (e.g. `c:\setup.exe /s`). The file `device.lock.ini` allows you to customize the installation parameters. This file must be in the same folder as `setup.exe`.

You can open and edit `device.lock.ini` in any text editor (for example, in Notepad). Remove the semicolon (;) before the parameter to assign a new value or leave it to assign the default value.

There are two sections (`[Install]` and `[Misc]`) in the file `device.lock.ini` and each section has its own parameters, as described in the sections that follow.

### **Section [Install]**

To install DeviceLock Service, specify the Service parameter:

`Service = 1`

You can also install DeviceLock management consoles and the documentation by using the `Manager` and `Documents` parameters.

To just upgrade DeviceLock Service without changing the existing settings, use the `OnlyUpgradeService` parameter:

`OnlyUpgradeService = 1`

In this case Setup ignores all specified settings and only upgrades DeviceLock Service to the new version.

You can also define the installation folder for DeviceLock:

`InstallDir = C:\Program Files\DeviceLock`

Setup uses this folder if it can't find the previous installation of DeviceLock.

If you have purchased licenses for DeviceLock, you can also specify the location of the license files:

`RegFileDir = C:\Directory`

where `C:\Directory` is where your license files are located.

You do not need to load the licenses, if you are installing only DeviceLock Service. They are required for DeviceLock management consoles and separately licensed components: ContentLock and NetworkLock.

To instruct DeviceLock Service to use a fixed port, specify the `FixedPort` parameter:

`FixedPort = [port number]`

where `port number` is the TCP port number to be used for communication between DeviceLock Service and management consoles. To use dynamic ports for the RPC communication, specify `0` as a port number. By default, DeviceLock Service uses port 9132.

If the `CreateGroups` parameter is set to 1, Setup creates the special local user group `Allow_Access_To_` for each device type (e.g. `Allow_Access_To_Floppy` for floppy drives), if these do not exist on the local computer.

To apply settings, permissions, audit, shadowing rules and alerts to DeviceLock Service, specify the path to the previously saved DeviceLock Service settings file in the `SettingsFile` parameter:

`SettingsFile = C:\settings.dls`

This settings file can be created using DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor.

### ***Section [Misc]***

To run a program after a successful install, set the `Run` parameter, e.g. `Run = C:\mybatchfile.bat`

To suppress an automatic restart even if Setup needs it, set `DisableRestart = 1`



## Installation via Microsoft Systems Management Server

**Unattended Installation** allows you to deploy DeviceLock Service using Microsoft Systems Management Server (SMS). Use the package definition files (DevLock.pdf for SMS version 1.x and DevLock.sms for SMS version 2.0 and later) supplied with DeviceLock, located in the sms.zip file.

## Installation via DeviceLock Management Console

DeviceLock Management Console (the MMC snap-in) supports remote installation to help system administrators set up a service on remote machines without ever having to physically go to them.

---

### Note

Only the built-in administrator account can be used to perform a remote installation of DeviceLock Service on computers running Windows Vista or a later version of Windows. In a Windows Active Directory environment, only members of the Domain Admins group can perform a remote installation of DeviceLock Service. Administrator privileges are required to connect to DeviceLock Service via DeviceLock Management Console. For more information, refer to Microsoft's article at [support.microsoft.com/kb/951016](https://support.microsoft.com/kb/951016).

---

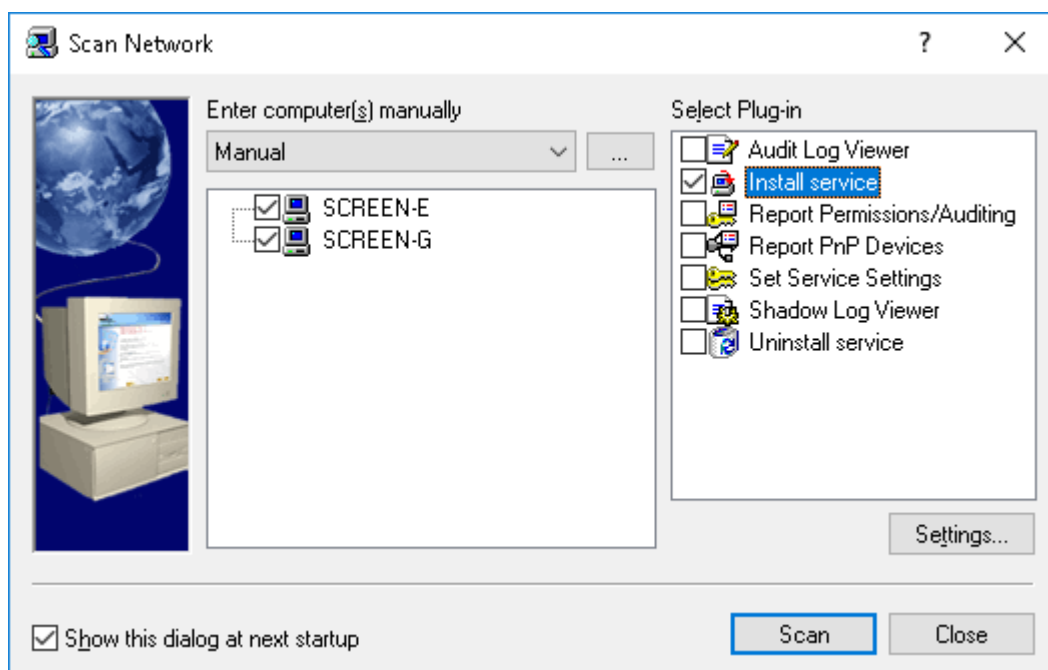
When you're trying to connect to a computer where DeviceLock Service is not installed or is outdated, the management console prompts you to install or update it. The following message appears: "Device Lock service does not exist on <computer name> Do you want to install it?"

Select the folder that contains all of the files needed for installation (such as DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe, and InstMsiW.exe). These files are located in the DeviceLock installation folder (%ProgramFiles%\DeviceLock by default).

By default, the DeviceLock Service installation files will be copied to the folder %ProgramFiles%\DeviceLock Agent if this service doesn't exist on this system. If the service exists on the system but its version is lower than 7.0, the management console will also copy the installation files to the default folder %ProgramFiles%\DeviceLock Agent. If the service exists on the system but its version is 7.0 or higher, the management console will copy the installation files to the folder containing the old files and the old files will be replaced.

## Installation via DeviceLock Enterprise Manager

DeviceLock Enterprise Manager contains the **Install service** plug-in that allows you to deploy DeviceLock Service automatically on all the selected computers in your network.

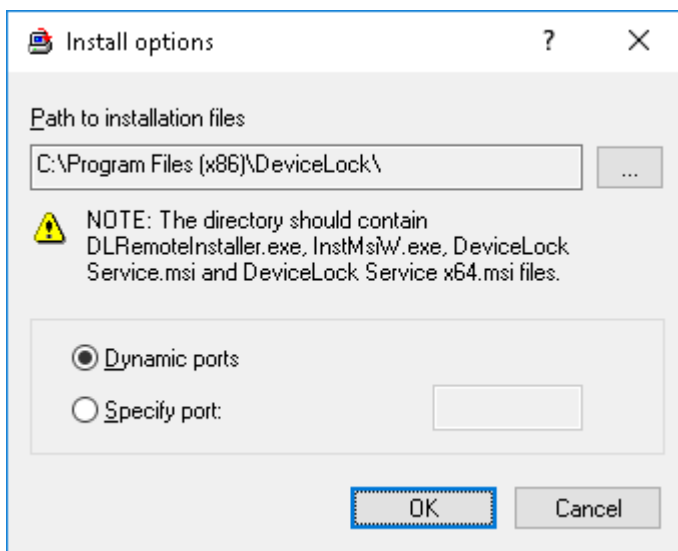


### Note

Only the built-in administrator account can be used to perform a remote installation of DeviceLock Service on computers running Windows Vista or a later version of Windows. In a Windows Active Directory environment, only members of the Domain Admins group can perform a remote installation of DeviceLock Service. Administrator privileges are required to connect to DeviceLock Service via DeviceLock Management Console. For more information, refer to Microsoft's article at [support.microsoft.com/kb/951016](https://support.microsoft.com/kb/951016).

First, select computers where DeviceLock Service must be installed. DeviceLock Enterprise Manager allows you to select computers by their types and names. You can also specify a list of computers by typing computer names or IP addresses, load a list of computers from an external file, or select computers from an LDAP-compatible directory (such as Active Directory, Novell eDirectory, OpenLDAP, etc.).

Then, select the **Install service** plug-in and click the **Settings** button to specify the folder that contains all of the files needed for installation (such as DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe, and InstMsiW.exe). These files are located in the DeviceLock installation folder (%ProgramFiles%\DeviceLock by default). You can also instruct DeviceLock Service to use the fixed TCP port for the communication with management consoles. To use dynamic ports for the RPC communication, select the **Dynamic ports** option. By default, DeviceLock Service uses port 9132.



By default, the DeviceLock Service installation files will be copied to the folder %ProgramFiles%\DeviceLock Agent if this service doesn't exist on this system. If the service exists on the system but its version is lower than 7.0, the **Install service** plug-in will also copy the installation files to the default folder %ProgramFiles%\DeviceLock Agent. If the service exists on the system but its version is 7.0 or higher, the **Install service** plug-in will copy the installation files to the folder containing the old files and the old files will be replaced.

## Installation via Group Policy

This step-by-step instruction describes how to use Group Policy to automatically distribute DeviceLock Service to client computers. DeviceLock Service can be deployed in an Active Directory domain using the Microsoft Software Installer (MSI) package DeviceLock Service.msi and DeviceLock Service x64.msi.

---

### Note

If you use a custom MSI package with defined DeviceLock Service settings to deploy DeviceLock Service using Group Policy, these settings are not applied to client computers if any one of the following conditions is true:

- The default security is disabled on remotely running DeviceLock Services.
- The GPO applied to client computers has the **Override Local Policy** setting enabled.

For information about how to create a custom MSI package, see [Create MSI Package](#).

---

You can use Group Policy to distribute DeviceLock Service by using the following steps:

- **Create a Distribution Point**

To install DeviceLock Service, you must create a distribution point on the server. To create a distribution point, do the following:

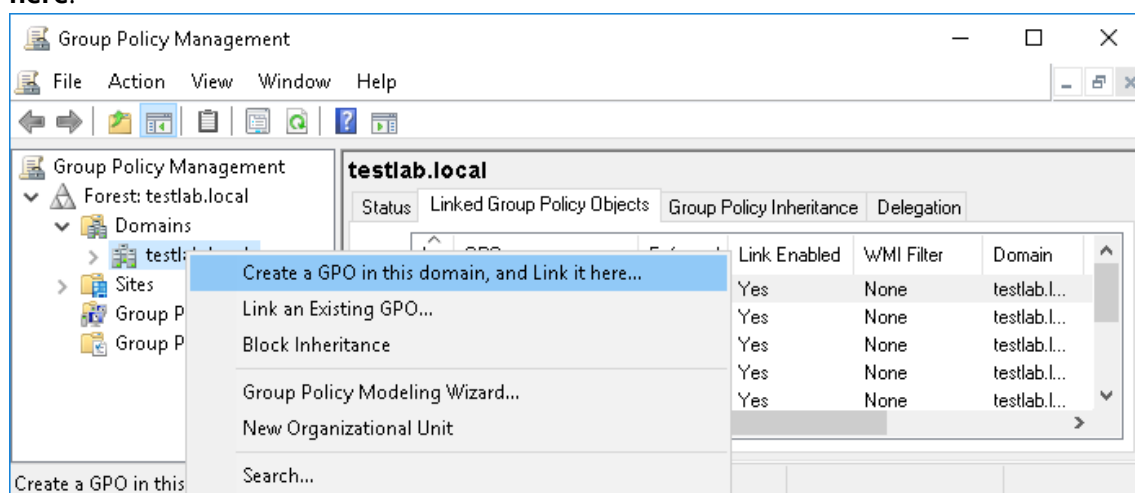
1. Log on to the server computer as an administrator.
2. Create a shared network folder in which to place the MSI package.

3. Set permissions on the share to allow access to the distribution package.
4. Copy the MSI package DeviceLock Service.msi and/or DeviceLock Service x64.msi to the distribution point.

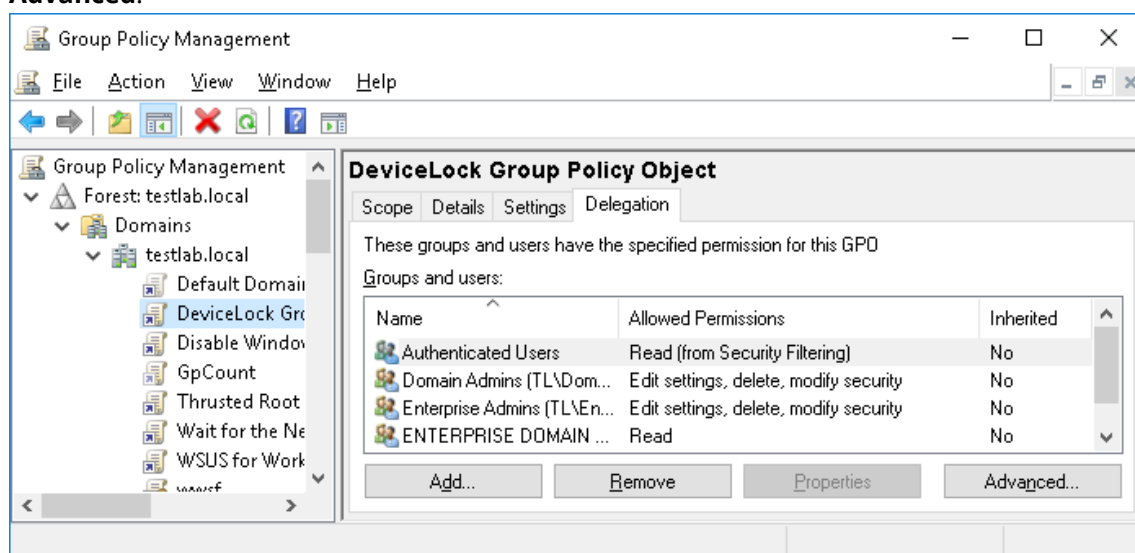
- **Create a Group Policy Object**

To create a Group Policy object (GPO) with which to distribute DeviceLock Service, do the following:

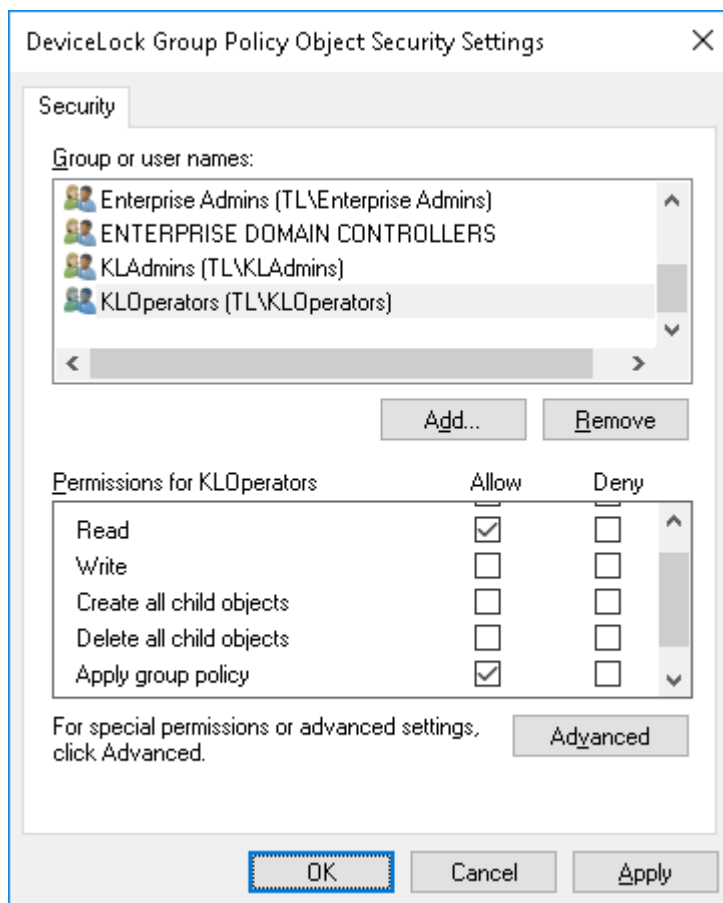
1. In the Group Policy Management console tree, right-click your domain and then select the following command from the shortcut menu: **Create a GPO in this domain, and Link it here.**



2. Type the name that you want to call this policy, and then press ENTER.
3. In the console tree, select your Group Policy object, click the **Delegation** tab, and then click **Advanced**.



4. In the **Security Settings** dialog box that appears, select the **Deny** check box next to **Apply group policy** for the security groups that you want to prevent from having this policy applied. Select the **Allow** check box for the groups to which you want to apply this policy.

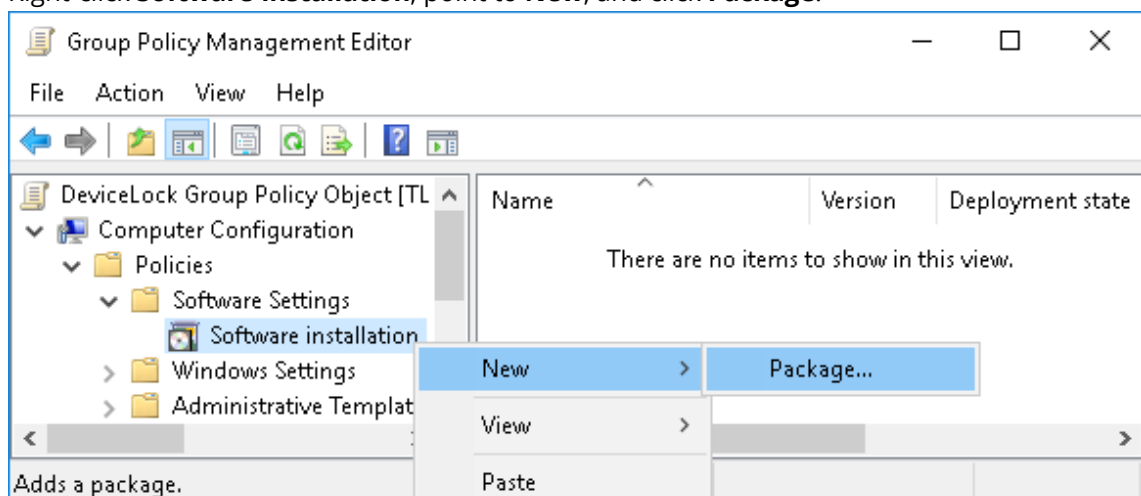


5. When you are done, click **OK**.

- **Assign a Package**

To assign DeviceLock Service to computers running Windows:

1. Use the Group Policy Management console to open the Group Policy object in the Group Policy Management Editor.
2. Under **Computer Configuration**, expand **Software Settings**.
3. Right-click **Software installation**, point to **New**, and click **Package**.



4. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path to the shared folder that contains the DeviceLock Service MSI package. For example:  
\\file server\share\DeviceLock Service.msi.

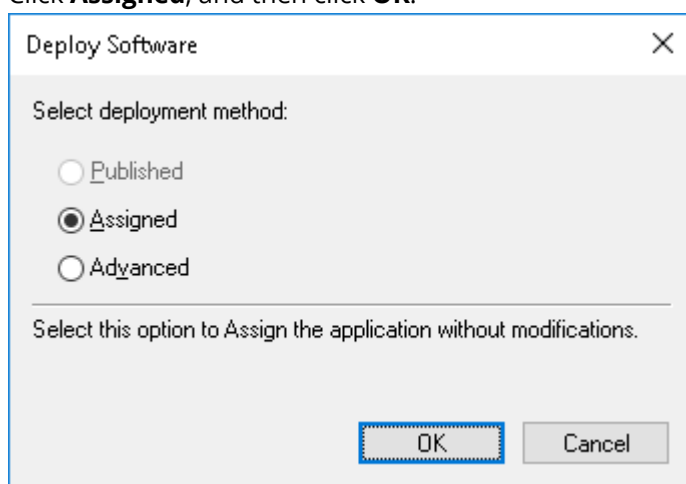
---

**Important**

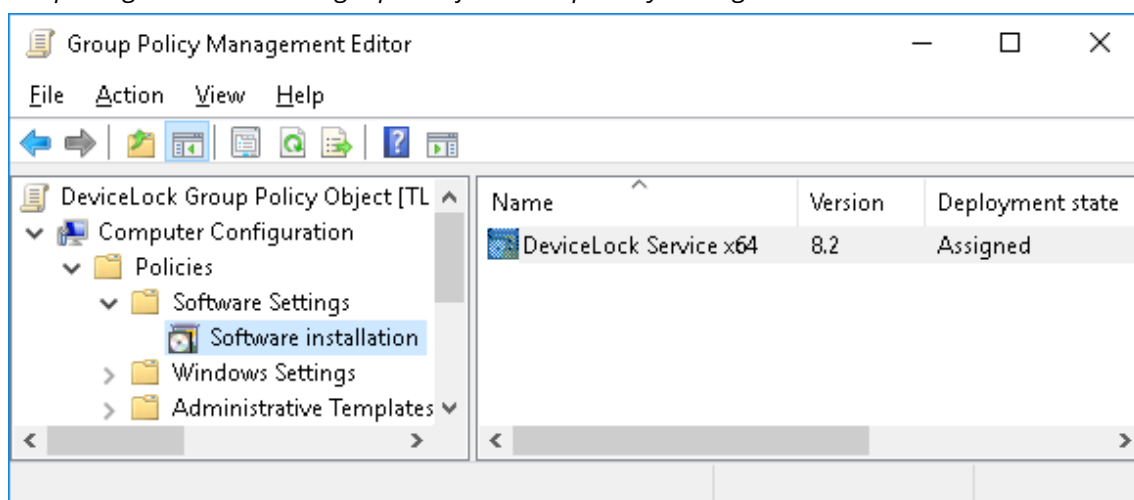
Do not browse to the location. Ensure that you use the UNC path to the shared folder.

---

5. Click **Open**.
6. Click **Assigned**, and then click **OK**.



The package is listed in the right pane of the Group Policy Management Editor window.



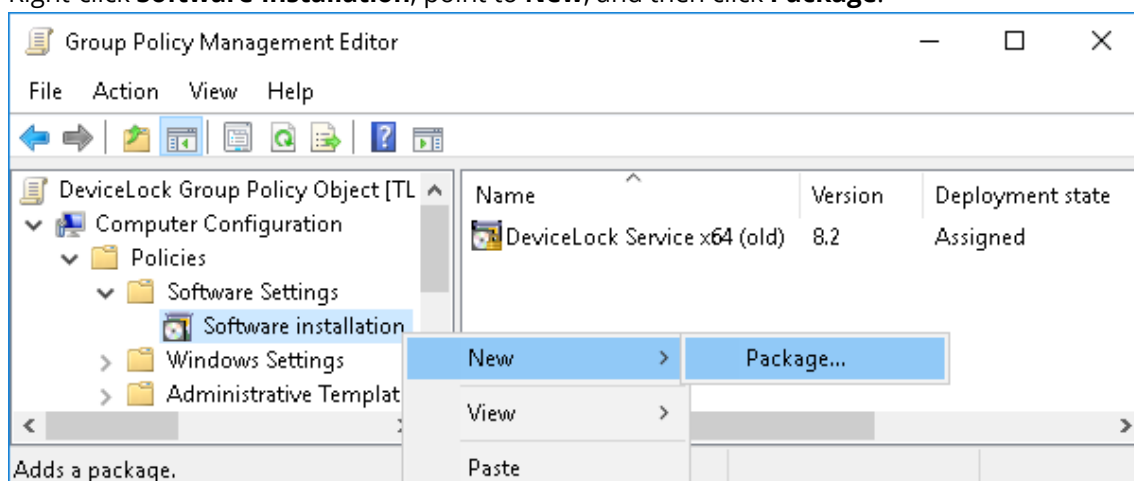
7. Close the Group Policy Management Editor. When the client computer starts, DeviceLock Service is automatically installed.

- **Upgrade a Package**

If the previous version of DeviceLock Service was already deployed and you want to upgrade it to the new one:

1. Use the Group Policy Management console to open the Group Policy object that contains the old DeviceLock Service package in the Group Policy Management Editor.
2. Under **Computer Configuration**, expand **Software Settings**.

3. Right-click **Software installation**, point to **New**, and then click **Package**.

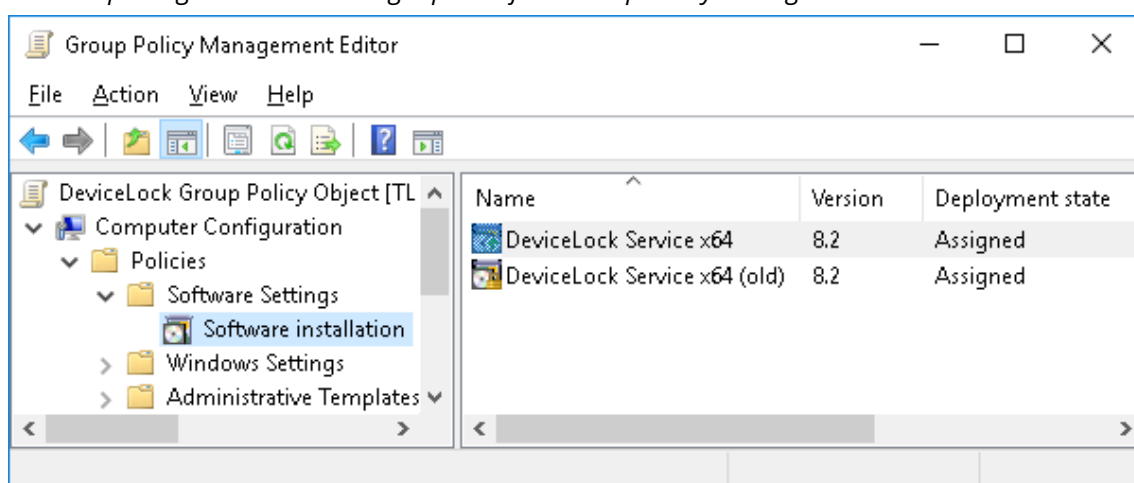


4. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path to the shared folder that contains the new DeviceLock Service MSI package. For example:

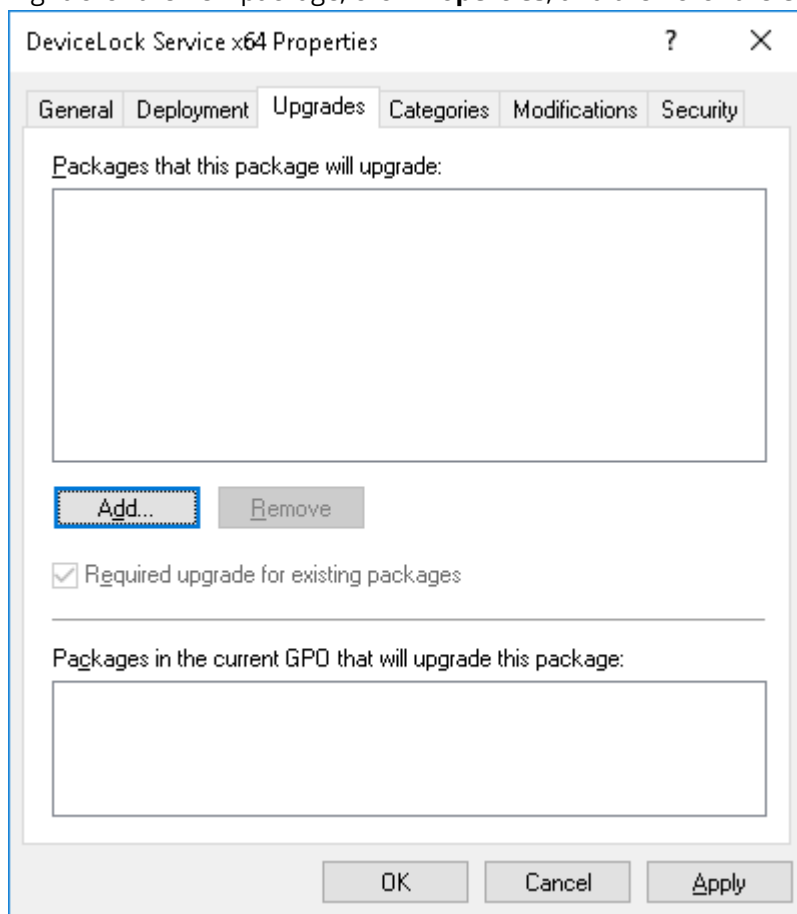
\\file server\share\DeviceLock Service.msi.

5. Click **Open**.
6. Click **Assigned**, and then click **OK**.

*The new package is listed in the right pane of the Group Policy Management Editor window.*

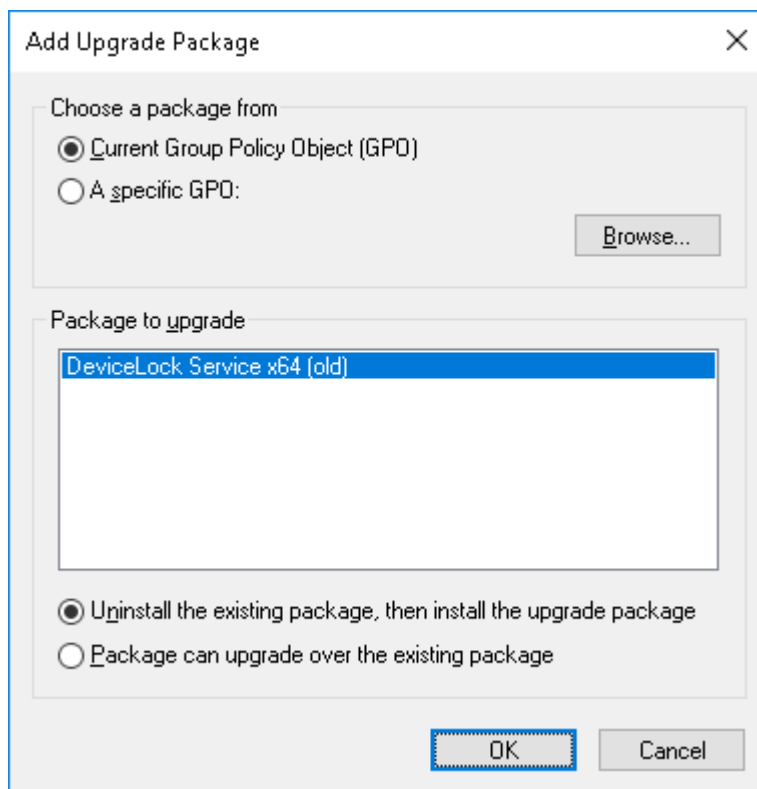


7. Right-click the new package, click **Properties**, and then click the **Upgrades** tab.



8. Click **Add**, select the old DeviceLock Service package you want to upgrade, choose the options **Uninstall the existing package, then install the upgrade package**, and then click **OK**.





9. Click **OK** to close the **Properties** dialog box. Then, close the Group Policy Management Editor. When the client computer starts, DeviceLock Service is automatically upgraded.

---

#### Note

Normally, when upgrading DeviceLock Service, the new MSI package detects the package to update in the GPO so the actions in Step 7 and Step 8 are performed automatically.

---

#### • Redeploy a Package

In some cases you may want to redeploy DeviceLock Service.

To redeploy a package:

1. Use the Group Policy Management console to open the Group Policy object which contains the deployed package in the Group Policy Management Editor.
2. Expand the **Software Settings** container that contains the **Software installation** item with which you deployed the package.
3. Click the **Software installation** container that contains the package.
4. In the right pane of the Group Policy Management Editor window, right-click the program, point to **All Tasks**, and then click **Redeploy application**.  
*The following message is displayed: "Redeploying this application will reinstall the application everywhere it is already installed. Do you want to continue?"*
5. Click **Yes**.
6. Close the Group Policy Management Editor.

#### • Remove a Package

To remove DeviceLock Service:

1. Use the Group Policy Management console to open the Group Policy object which contains the deployed package in the Group Policy Management Editor.
2. Expand the **Software Settings** container that contains the **Software installation** item with which you deployed the package.
3. Click the **Software installation** container that contains the package.
4. In the right pane of the Group Policy Management Editor window, right-click the program, point to **All Tasks**, and then click **Remove**.
5. Click **Immediately uninstall the software from users and computers**, and then click **OK**.
6. Close the Group Policy Management Editor.

Please be aware that:

- Deployment occurs only when the computer starts up, not on a periodic basis. This prevents undesirable results, such as uninstalling or upgrading an application that is in use.
- DeviceLock Service will be copied to the folder %ProgramFiles%\DeviceLock Agent if this service doesn't exist on the system. If the service exists on the system but its version is lower than 7.0, DeviceLock Service will also be copied to the default folder %ProgramFiles%\DeviceLock Agent. If the service exists on the system but its version is 7.0 or higher, DeviceLock Service will be copied to the folder containing the old version and the old version will be replaced.

## Installation via DeviceLock Enterprise Server

You can use monitoring tasks in DeviceLock Enterprise Server to automatically distribute DeviceLock Service to client computers. DeviceLock Service can be deployed from the Microsoft Software Installer (MSI) package DeviceLock Service.msi or DeviceLock Service x64.msi.

---

### Note

If the DeviceLock Enterprise Server service is configured to run under the Local System account, Monitoring tasks cannot install, update or remove DeviceLock Service from remote computers.

---

For instructions on how to create a monitoring task, see [Create/Edit Task](#).

To configure the task to install DeviceLock Service, select the **Install/Update DeviceLock Service automatically** check box in the **Create Task** dialog box, and make sure that the **Active** check box is selected.

**Create Task**

Name:

☒ Active

Computers:

Network discovery methods:

☐ Ping sweep

☒ NetBIOS queries

☐ TCP djscovery (ports):

Service connection settings:

☒ Dynamic ports

☐ Fixed TCP port:

☒ Verify Service Settings:

Service Settings file:

☐ Restore Service Settings

Scanning interval:    sec

Number of scanning threads:

☒ Install/Update DeviceLock Service automatically

☐ Remove DeviceLock Service automatically

To configure the task to uninstall DeviceLock Service, select the **Remove DeviceLock Service automatically** check box.

DeviceLock Enterprise Server installs and removes DeviceLock Service when executing monitoring tasks configured that way.

---

**Note**

If you use a custom MSI package with defined DeviceLock Service settings to deploy DeviceLock Service using DeviceLock Enterprise Server, these settings are not applied to client computers if any one of the following conditions is true:

- The name of the MSI package is different from DeviceLock Service.msi or DeviceLock Service x64.msi.
- The first 3 digits of DeviceLock Service version number do not match those of DeviceLock Enterprise Server.

For information about how to create a custom MSI package, see [Create MSI Package](#).

---

## Deploying DeviceLock Service for Mac

To deploy DeviceLock for Mac, use the installer file DeviceLock Service.pkg from the appropriate image included with the DeviceLock distribution package.

First, you need to mount the image file DeviceLock Service.dmg.

Next, you can use the following ways to install DeviceLock Service for Mac from that image:

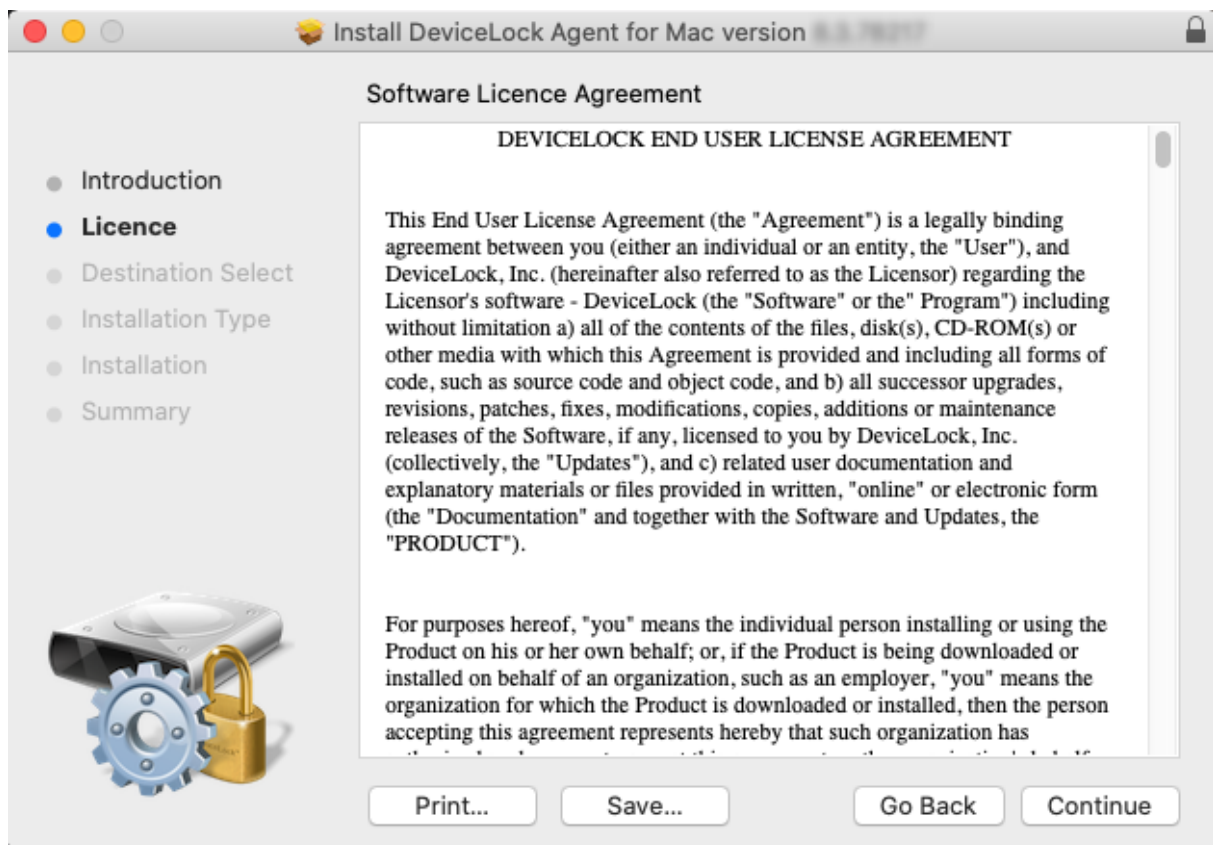
- [Interactive Installation](#)
- [Command Line Utility](#)
- [Unattended Installation](#)

### Interactive Installation

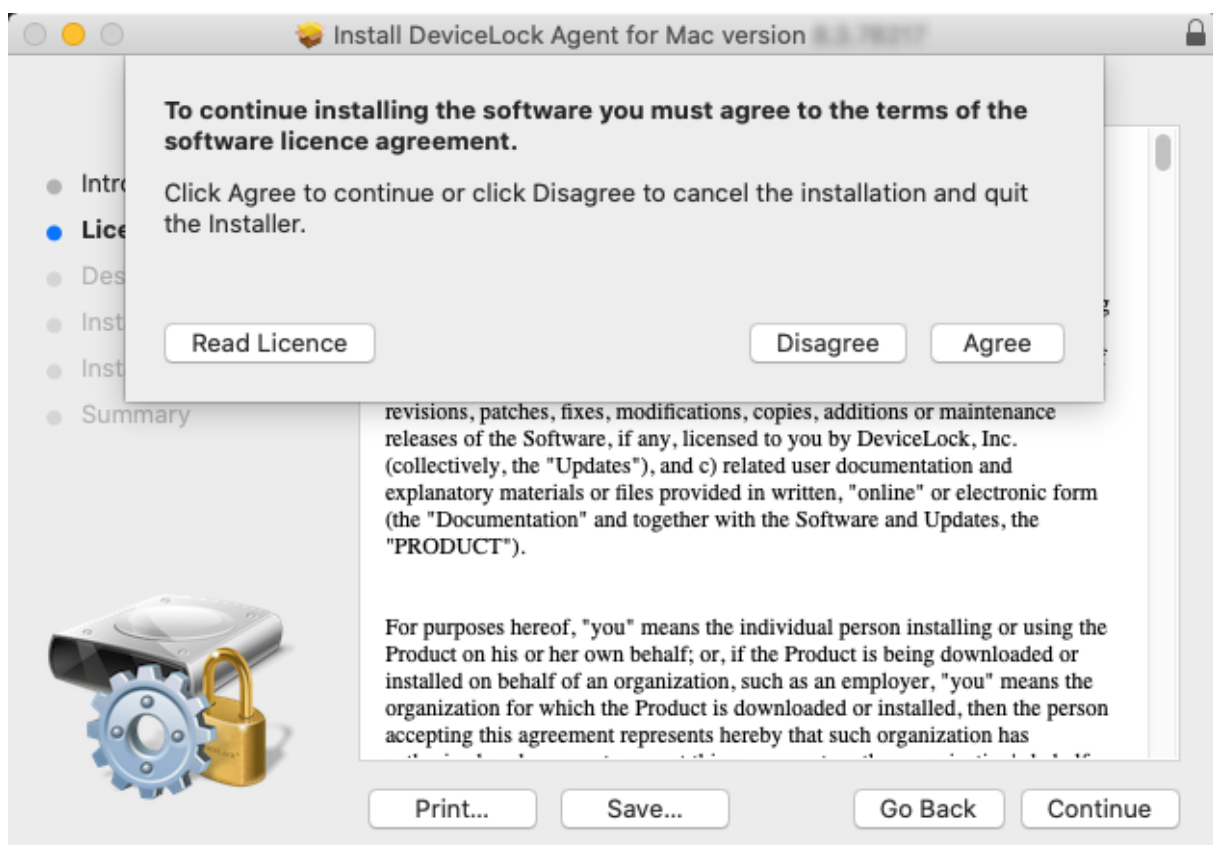
Interactive installation is engaged by launching the installer file DeviceLock Service.pkg. You should run DeviceLock Service.pkg on each computer that is to be controlled with DeviceLock Service for Mac. If you are upgrading a previous version, make sure that you have administrative access to DeviceLock Service for Mac; otherwise you will not be able to continue installation.

To install DeviceLock Service for Mac in interactive mode, launch DeviceLock Service.pkg and follow the instructions that appear on the screen.

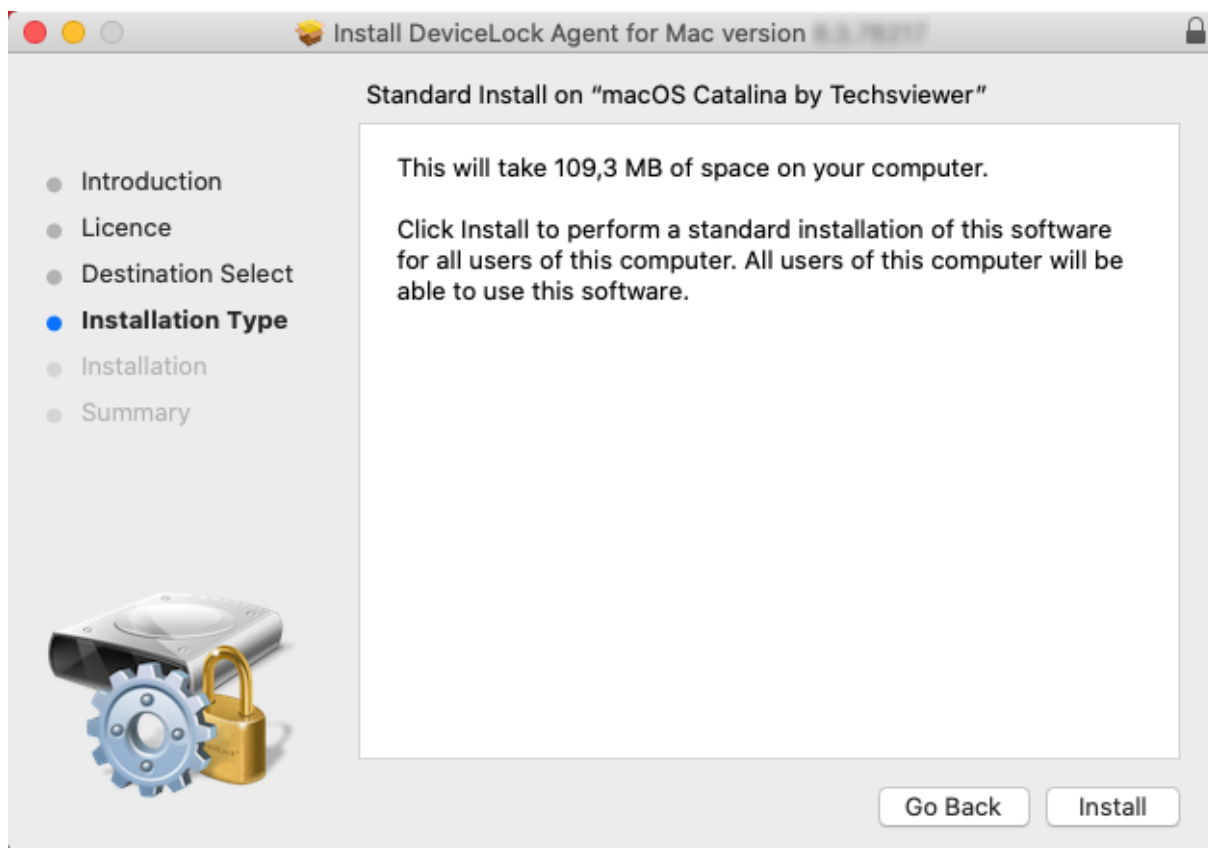
You will be presented with DeviceLock End User License Agreement. You may print or save the text of this License Agreement for future reference. Click **Continue** to proceed to the next step.



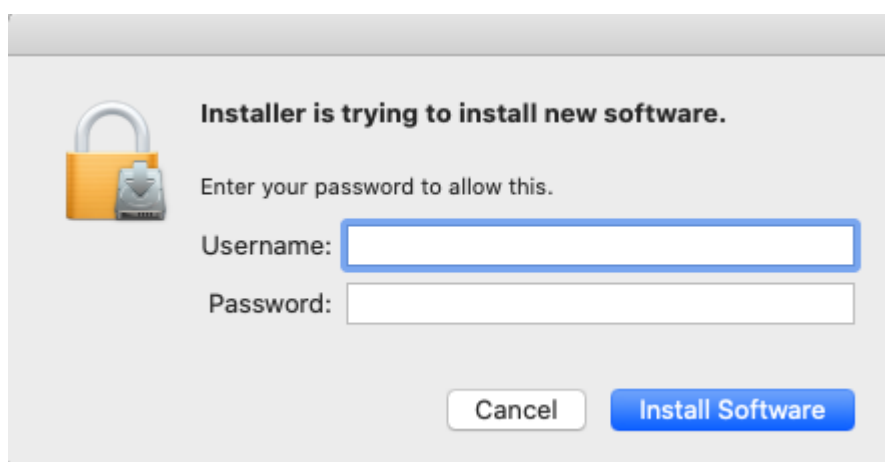
You will need to read and accept DeviceLock End User License Agreement before continuing installation. Click **Agree** to proceed to the next step.



You will be informed on the amount of disk space required for installing DeviceLock Service for Mac. At this point, DeviceLock Service for Mac is ready to be installed. Click **Install** to continue.



You will need to authenticate with administrative credentials in order to be able to install DeviceLock Service for Mac. Enter user name and password of a user having administrative privileges, and click **Install Software** to continue.



A dialog window with a progress bar will be displayed. The installation may take several minutes. You cannot interrupt DeviceLock Service for Mac installation. Should you need to uninstall the product later on, please follow the standard software uninstallation procedure.

After a few minutes, the installation is complete. Click **Close** to close the installer.

## Command Line Utility

Installation is also possible by using a command-line utility. This utility can install DeviceLock Service for Mac in interactive or unattended mode. Do note, however, that you will need to have administrative access to the computer you will be installing DeviceLock Service for Mac on.

The command line utility is located at `/Library/DeviceLockAgent/Utilities/install`. The utility can be placed (copied) to any other location. A single `.pkg` file should be placed along with this utility in the same location. It is essential to only place a single `.pkg` file; otherwise, if running the installation tool without parameters, a random package may be installed.

The command line tool can work in either interactive or unattended (silent) mode. Use the command line utility to install DeviceLock Service for Mac as follows.

While there are several ways to install DeviceLock Service for Mac, making use of the following command is recommended:

```
sudo install --delayed --package <path_to_package> --settings <path_to_ini_file>
```

The `--settings` parameter is optional.

For example:

```
sudo /Volumes/DeviceLock/Utilities/install --delayed --package  
/Volumes/DeviceLock/DeviceLockAgent.pkg --settings /Users/admin/devicelock.ini
```

---

### Note

If the computer on which you are installing DeviceLock Service for Mac runs Python 3 or older, use the following command:

```
sudo python2.7 install --delayed --package <path_to_package> --settings <path_to_ini_file>
```

- OR -

```
sudo python2.6 install --delayed --package <path_to_package> --settings <path_to_ini_file>
```

By default, Apple distributes its systems with Python 2.6 or 2.7.

---

If DeviceLock Service for Mac is being installed for the first time, the above command will launch silent (unattended) installation. Otherwise, the system will update or reinstall DeviceLock Service for Mac upon computer reboot.

When reinstalling or upgrading DeviceLock Service for Mac, interactive installation is not recommended as the updated service will start working only after reboot.

## Unattended Installation

To install DeviceLock Service for Mac without user intervention, you will need using the command line installation tool in the silent mode.

Unattended installation is performed by running the installation tool with the parameter `--silent` or `--delayed` in the command line. The `--delayed` parameter also implies `--silent`. Note that depending on whether or not the “root” user appears in the list of DeviceLock Administrators, the installation tool will exhibit different behavior:

- If the installation utility is launched without specifying a `.pkg` file, it will install the first `.pkg` file located in the same directory where the tool is located. If there are several `.pkg` files in that directory, a random one may be installed.
- A specific `.pkg` file can be used by appending the full file name after the `--package` key. The keys can be used in any order. Relative file names are supported.
- Finally, the installation utility will perform a silent install if “root” is not included in the list of DeviceLock Administrators. If this is the case, the installation tool will copy the `.pkg` file into the `/Library/DeviceLockPackages` directory. The service will reinstall or update on next reboot.

You can configure DeviceLock Service for Mac automatically immediately after installation. To pre-configure DeviceLock Service for Mac during installation, edit the file `devicelock.ini` by adding the path to the `.dls` settings file. You can use a local or network path.

For example:

```
sudo /MyDirectory/install --silent --package /SomeDir/DeviceLock.pkg --settings  
/SomeDir/devicelock.ini
```

---

#### Note

The format of the file `devicelock.ini` for Mac is the same as for Windows (see [Unattended Installation](#) for Windows), with the difference that only the `SettingsFile` parameter is in effect. This parameter specifies the path and name of the settings file (`.dls`) to be used to configure DeviceLock Service just following the installation.

---

## Installing Management Consoles

DeviceLock management consoles are the control interfaces that systems administrators use to remotely manage DeviceLock Service, DeviceLock Enterprise Server and DeviceLock Content Security Server.

Install the DeviceLock management consoles on the computer from which the administrator is going to manage DeviceLock settings and run reports. It is not necessary to install management consoles on the server (domain controller or others), even if you are going to use DeviceLock Group Policy Manager to manage settings via Active Directory Group Policy - you can do it from your local workstation (proper privileges required).

---

#### Note

DeviceLock Group Policy Manager integrates into Windows Group Policy Editor and is not available as a stand-alone application. In order to use DeviceLock Group Policy Manager, you must run the standard Windows Group Policy Editor.

---

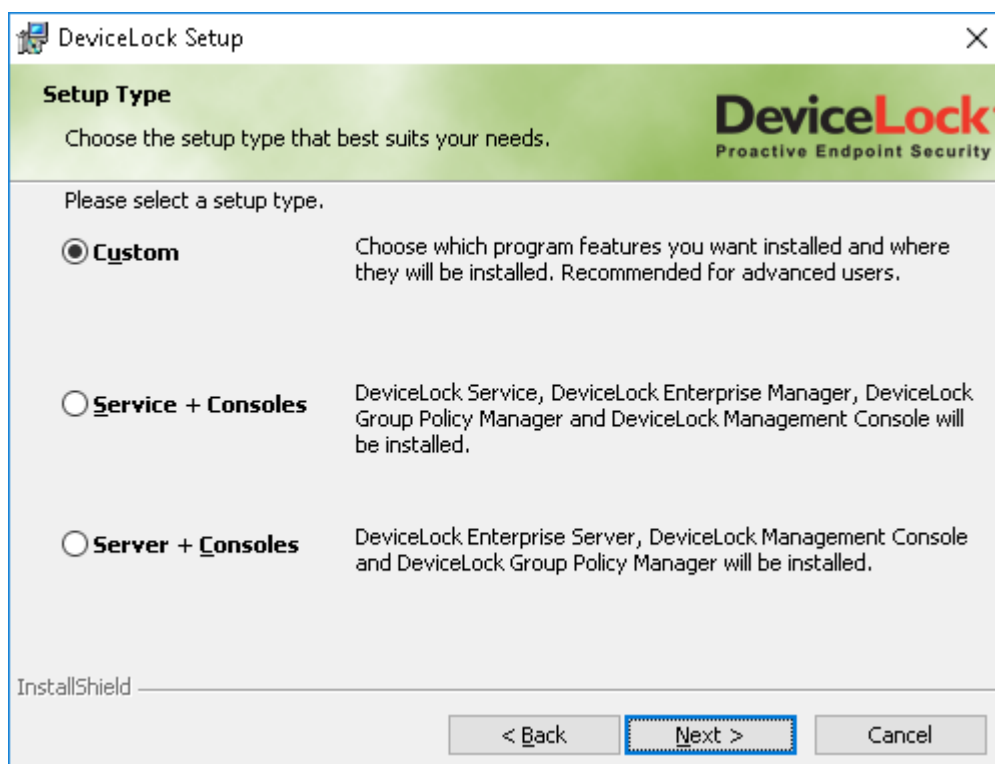


Run the Setup program (setup.exe) and follow the instructions on the wizard pages that appear on the screen.

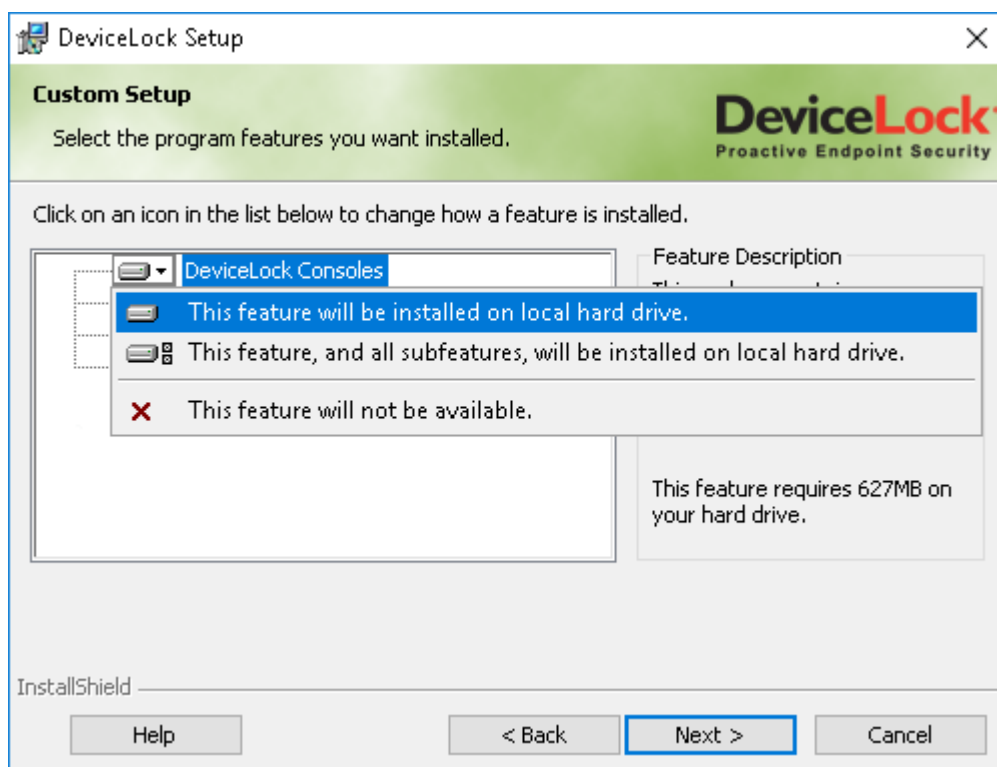
On the **License Agreement** page, read the License Agreement and then click **I accept the terms in the license agreement** to accept the licensing terms and conditions and proceed with the installation.

On the **Customer Information** page, type your user name and organization.

On the **Setup Type** page, select the required setup type.



You have the following three choices: install both DeviceLock Service and DeviceLock management consoles using the **Service + Consoles** option, install both DeviceLock Enterprise Server and DeviceLock management consoles using the **Server + Consoles** option or install only DeviceLock management consoles using the **Custom** option and selecting the **DeviceLock Consoles** component.



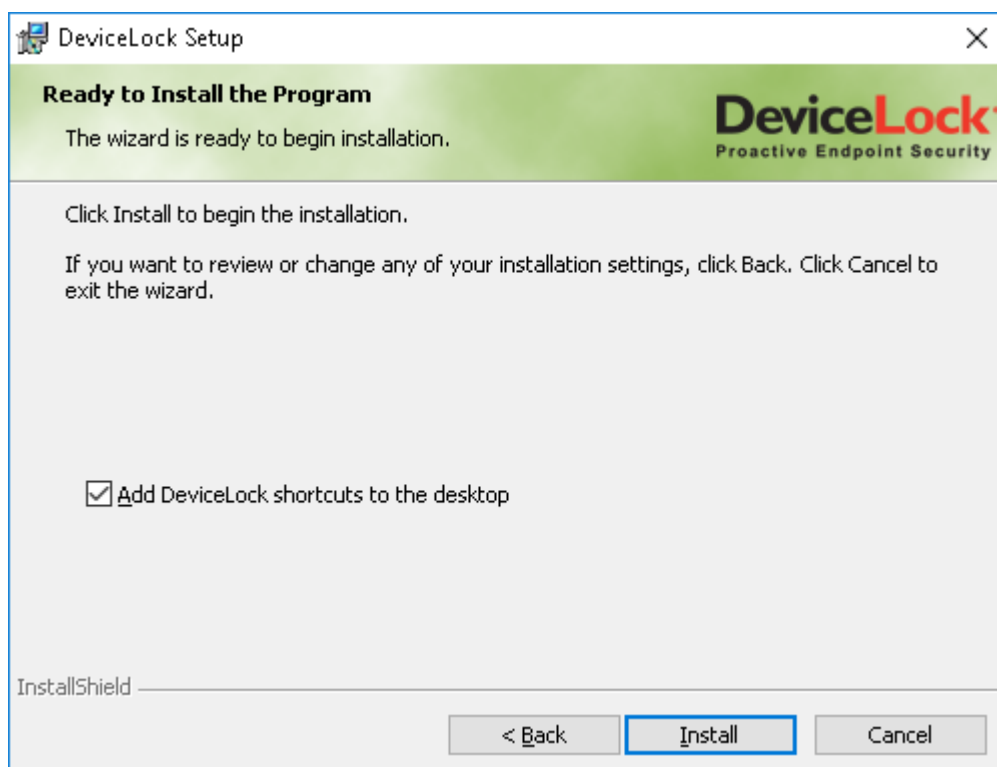
## Note

On the **Custom Setup** page, you can select the RSoP component to install. This component enables support for DeviceLock's Resultant Set of Policy planning mode on domain controllers. The RSoP component is required only when DeviceLock management consoles are installed, but DeviceLock Service is not installed on the computer. For more information on RSoP planning mode, refer to Microsoft's documentation at [technet.microsoft.com/library/cc758010.aspx](https://technet.microsoft.com/library/cc758010.aspx).

On the **Custom Setup** page, you can change the default installation folder. Click **Change** and then choose a folder in the dialog box that appears. The default folder is %ProgramFiles%\DeviceLock.

DeviceLock ships with three different management consoles: DeviceLock Management Console, DeviceLock Enterprise Manager, and DeviceLock Group Policy Manager (integrates into the Windows Group Policy Editor). Installed together with other management consoles is DeviceLock Service Settings Editor, a tool used for creating and modifying external files with settings, permissions, audit, shadowing rules and alerts for DeviceLock Service (DeviceLock Service settings files).

On the **Ready to Install the Program** page, click **Install** to begin the installation. Select the **Add DeviceLock shortcuts to the desktop** check box if you want to add DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Service Settings Editor shortcuts to the desktop.



Setup may suggest that you generate a new DeviceLock Certificate. The following message will appear: “Do you want to create the new DeviceLock Certificate (the private and public key pair)? Click “No” if you already have DeviceLock Certificate and you don’t need to create the new key pair.”

You can always generate the new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just click the **No** button and continue the installation. For more information on DeviceLock Certificates, see the [DeviceLock Certificates](#) section later in this document.

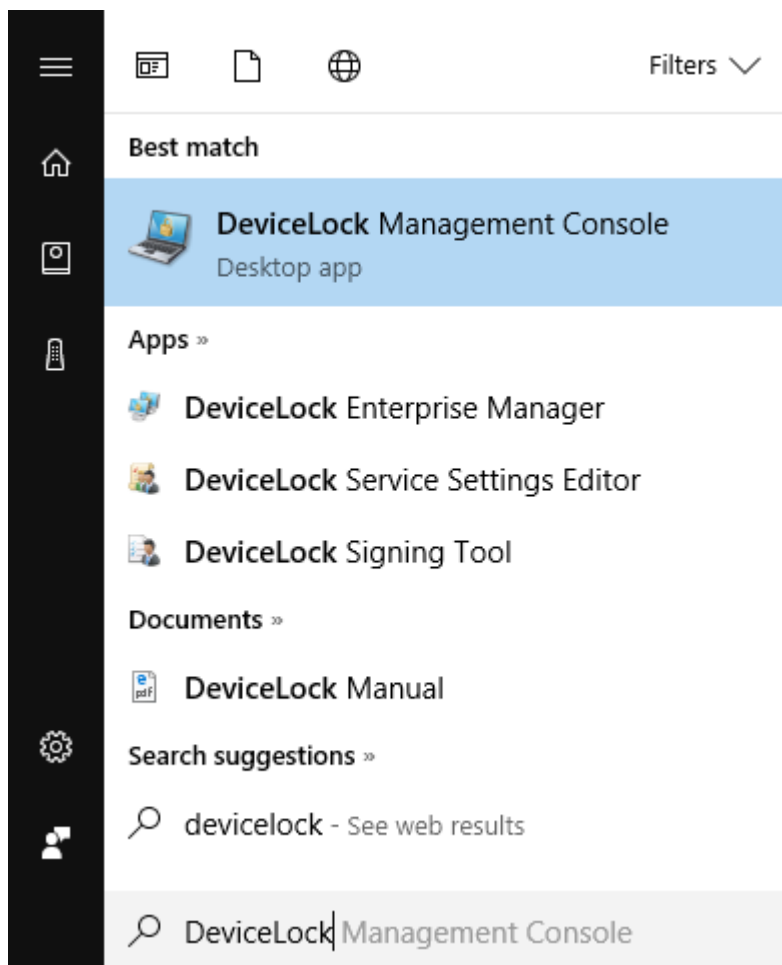
Also, Setup may suggest that you load the license files for DeviceLock. If you don’t have the license files, click **Cancel** to install DeviceLock in a 30-day trial mode. For more information, see [Activating Client Licenses](#).

If you opted to install DeviceLock Service as well, Setup suggests that you set special permissions for local devices and protocols. Click **Skip** if you prefer to wait until after installation to set permissions for devices and protocols using DeviceLock management consoles. For more information about these settings, refer to the [Interactive Installation](#) instructions for DeviceLock Service earlier in this document.

If you opted to install DeviceLock Enterprise Server as well, Setup suggests that you define its settings using the configuration wizard. For information about these settings, refer to the [Installation Steps](#) instructions for DeviceLock Enterprise Server later in this document.

On the **Installation Wizard Completed** page, click **Finish** to complete the installation. On this page, you will have the option to go to the DeviceLock home page. This option is selected by default.

You can run DeviceLock management consoles from the Windowsstart page.



---

### Note

You can uninstall DeviceLock as follows:

- Use **Programs and Features** in Control Panel (**Add or Remove Programs** on earlier versions of Windows) to remove **DeviceLock**.  
- OR -
  - Select **Remove DeviceLock** on the Windows **Start** menu.
- 

## Installing DeviceLock Enterprise Server

DeviceLock Enterprise Server is an optional component for centralized collection and storage of shadow data and audit logs. Also, DeviceLock Enterprise Server can monitor remote computers in real-time, checking DeviceLock Service status (running or not), policy consistency and integrity.

You can install several DeviceLock Enterprise Servers on different computers across your network for network load balancing.

DeviceLock Enterprise Server stores its data on a database server. Hence, a database server must be up and running on your network before installing DeviceLock Enterprise Server. For example, you could use Microsoft SQL Server Express Edition available for free download from Microsoft's website at [go.microsoft.com/fwlink/?LinkID=799012](https://go.microsoft.com/fwlink/?LinkID=799012).

It is not required to run the database server on the computer running DeviceLock Enterprise Server. Moreover, for performance and reliability reasons, it is better to run DeviceLock Enterprise Server on a separate computer.

There are three options for connecting DeviceLock Enterprise Server and the database server. Before installing DeviceLock Enterprise Server, decide which option best suits your needs:

1. **ONE-TO-ONE** - Installing one DeviceLock Enterprise Server and connecting it to one database server. This option is most appropriate for small networks (up to several hundred computers).
2. **MANY-TO-MANY** - Installing several DeviceLock Enterprise Servers and connecting each to its own database server. This option is typical for medium and large networks geographically distributed across a variety of segments.
3. **MANY-TO-ONE** - Installing several DeviceLock Enterprise Servers and connecting them all to a single database server. This option could be used for medium and large networks with a powerful (large amount of memory and free storage space) dedicated database server.

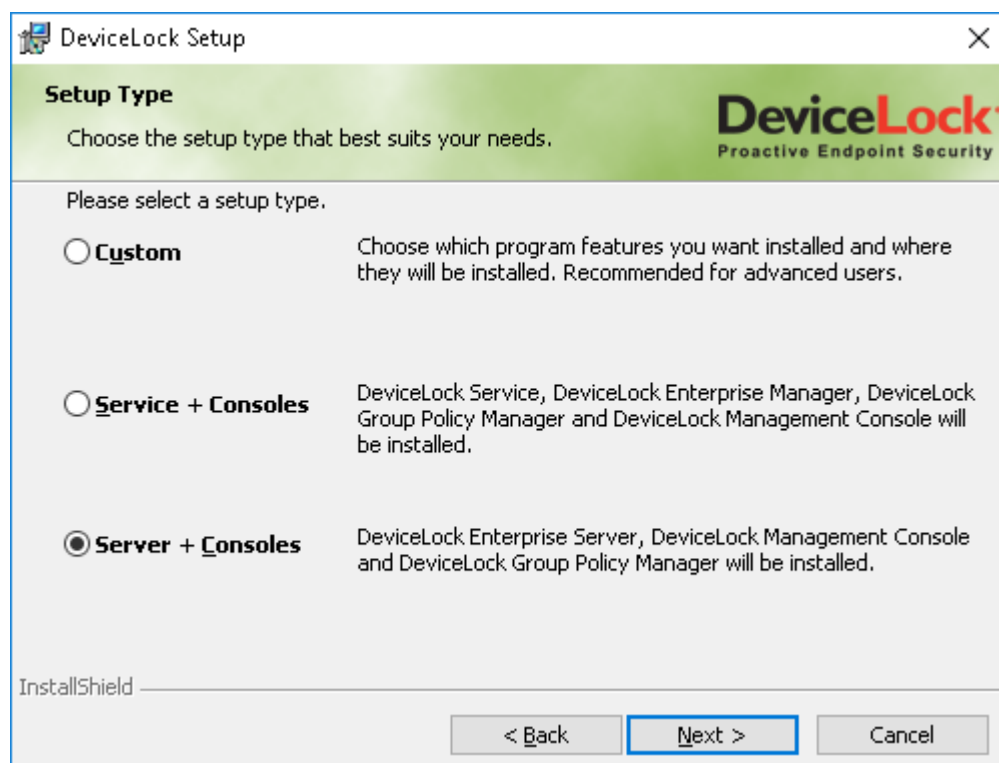
## Installation Steps

On each computer where your going to install DeviceLock Enterprise Server, setup.exe and follow the steps in the installation wizard that appears.

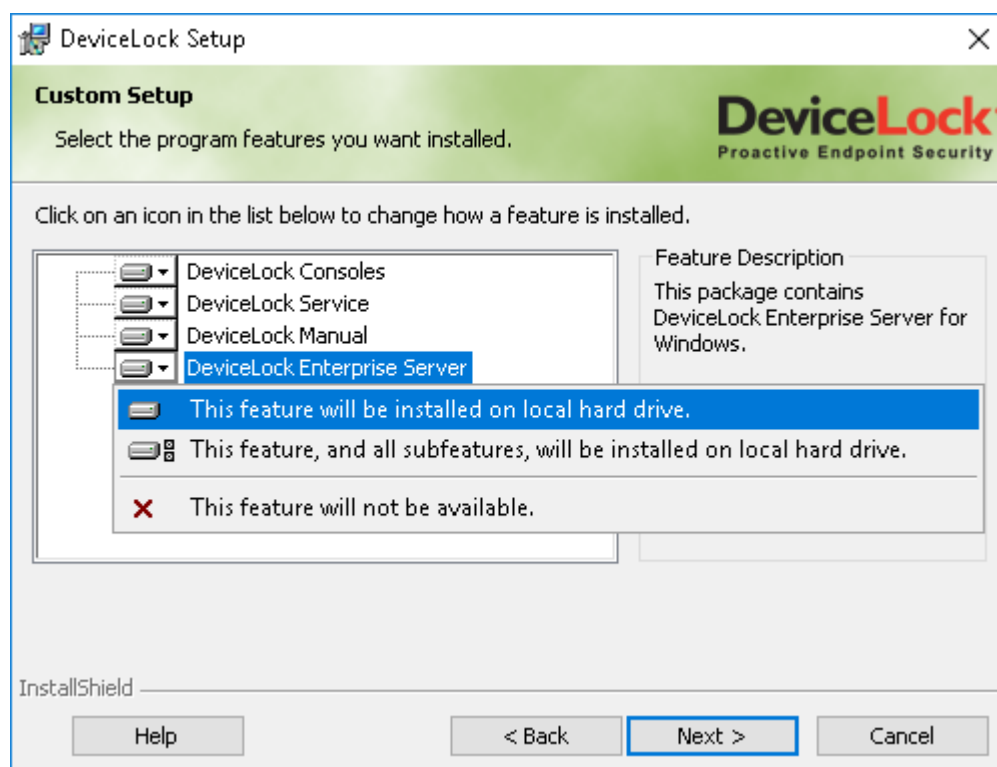
On the **License Agreement** page, read the License Agreement and then click **I accept the terms in the license agreement** to accept the licensing terms and conditions and proceed with the installation.

On the **Customer Information** page, type your user name and organization.

On the **Setup Type** page, select the required setup type.



You have the following two choices: either install both DeviceLock Enterprise Server and DeviceLock management consoles using the **Server + Consoles** option or install only DeviceLock Enterprise Server using the **Custom** option and selecting the **DeviceLock Enterprise Server** component.

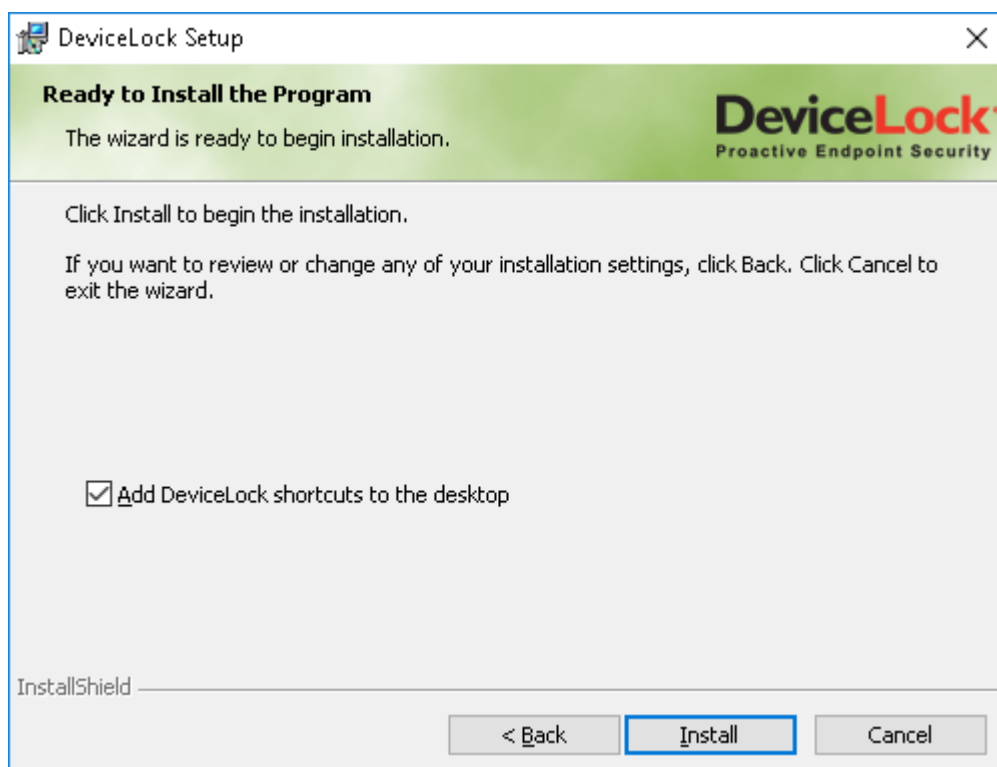


#### Note

On the **Custom Setup** page, you can select the RSoP component to install. This component enables support for DeviceLock's Resultant Set of Policy planning mode on domain controllers. The RSoP component is required only when DeviceLock management consoles are installed, but DeviceLock Service is not installed on the computer. For more information on RSoP planning mode, refer to Microsoft's documentation at [technet.microsoft.com/library/cc758010.aspx](https://technet.microsoft.com/library/cc758010.aspx).

On the **Custom Setup** page, you can change the default installation folder. Click **Change** and then choose a folder in the dialog box that appears. The default folder is %ProgramFiles%\DeviceLock.

On the **Ready to Install the Program** page, click **Install** to begin the installation. Select the **Add DeviceLock shortcuts to the desktop** check box if you want to add DeviceLock Management Console (the MMC snap-in), DeviceLock Enterprise Manager and DeviceLock Service Settings Editor shortcuts to the desktop.



If you selected to install DeviceLock management consoles as well, Setup may suggest that you generate a new DeviceLock Certificate. The following message will appear: "Do you want to create the new DeviceLock Certificate (the private and public key pair)? Click "No" if you already have DeviceLock Certificate and you don't need to create the new key pair."

You can always generate the new DeviceLock Certificate later, using the Certificate Generation Tool installed with DeviceLock management consoles. Hence, if at this step you are not sure whether you need the new certificate or not, just click the **No** button and continue the installation. For more information on DeviceLock Certificates, see the [DeviceLock Certificates](#) section later in this document.

If Setup detects that SQL Server is not running on the local computer but its installation package is available, Setup suggests that you run the SQL Server installation. The following message will appear: "SQL Server is not running on the local computer. Do you want to install it?"

If you don't want to install SQL Server on the local computer or it is already installed but just not started, click the **No** button.

During the installation process, you must configure DeviceLock Enterprise Server and define its main settings using the special wizard.

If you are installing an upgrade or simply reinstalling DeviceLock Enterprise Server and want to keep its current configuration, you don't need to go through this wizard again - just click **Next** and then **Cancel** to close the wizard and keep all existing settings unchanged.

In case you need to change some parameters but keep others - edit only needed parameters and go through all the wizard's pages up to the **Finish** button on the very last page.

## Note

If you are installing DeviceLock Enterprise Server for the first time (there are no existing settings on this computer yet) and you cancel the configuration wizard upon opening, Setup will not be able to install DeviceLock Enterprise Server's service, so you'll need to run the configuration wizard again. The following message will appear: "The wizard was interrupted before DeviceLock Enterprise Server could be completely installed. Do you want to run the wizard again (click "No" to continue this installation process without configuring DeviceLock Enterprise Server)?" If you click the **No** button to continue without installing DeviceLock Enterprise Server's service, you will need to run Setup later and install the service anyway.

## Service account and connection settings

On the first page of the configuration wizard you can specify the service startup account and TCP port for DeviceLock Enterprise Server.

DeviceLock Enterprise Server

Log on as

☐ Local System account

☒ This account: SCREEN-E\admin Browse...

Password: .....

Confirm password: .....

**NOTE:** We strongly recommend running DeviceLock Enterprise Server under an account in the Domain Admins group. DeviceLock Enterprise Server must have administrative access to every computer that is trying to connect to it.

Connection settings

☒ Dynamic ports

☐ Fixed TCP port:

< Back Next > Cancel

## Log on as

First of all, you should choose an account under which the DeviceLock Enterprise Server's service will start. As many other Windows services, the DeviceLock Enterprise Server's service can start under the special local system account (the SYSTEM user) and on behalf of any user.

To start the service under the SYSTEM user, select the **Local System account** option. Keep in mind that the process working under the SYSTEM user can't access shared network resources and authenticates on remote computers as an anonymous user. Therefore, DeviceLock Enterprise



Server configured to run under the SYSTEM user is not able to store shadow files on the remote computer (e.g. on the file server) and it must use DeviceLock Certificate for authentication on DeviceLock Services running on remote computers.

For more details on authentication methods, see the [Certificate Name](#) parameter description.

---

**Note**

If the DeviceLock Enterprise Server service is configured to run under the Local System account, you cannot install, update or remove DeviceLock Services on remote computers using a Monitoring task on DeviceLock Enterprise Server.

---

To start the service on behalf of the user, select the **This account** option, enter the user's account name and the password. It is recommended to use a user account that has administrative privileges on all the computers where DeviceLock Service is running. Otherwise, you will need to use DeviceLock Certificate authentication.

If you're installing DeviceLock Enterprise Server in the domain environment, we recommend that you use a user account that is a member of the Domain Admins group. Since Domain Admins is a member of the local group Administrators on every computer in the domain, members of Domain Admins will have full access to DeviceLock Service on every computer.

Also, don't forget that if DeviceLock Security is enabled on remotely running DeviceLock Services to protect them against local users with administrative privileges, the user's account specified in the **This account** option must be also in the list of DeviceLock Administrators with **Full access** rights. Otherwise, you'll need to use DeviceLock Certificate authentication.

**Connection settings**

You can instruct DeviceLock Enterprise Server to use a fixed TCP port for communication with the management console, making it easier to configure a firewall. Type the port number in **Fixed TCP port**. To use dynamic ports for RPC communication, select the **Dynamic ports** option. By default, DeviceLock Enterprise Server uses the 9133 port.

**Starting the service**

Click the **Next** button to start the DeviceLock Enterprise Server's service and to proceed to the second page.

If the current user doesn't have full administrative access to DeviceLock Enterprise Server (in case it already exists and you're installing an upgrade), the configuration wizard will not be able to install the service and apply changes. The following message will appear: "Access is denied." Also, the similar error may occur when the current user doesn't have local administrative privileges on the computer where DeviceLock Enterprise Server is installing.

If you've specified an incorrect user name for the **This account** option or the wrong user password, DeviceLock Enterprise Server will not be able to start. The following message will appear: "The account name is invalid or does not exist, or the password is invalid for the account name specified."

You will be notified if the user's account specified for the **This account** option is not a member of the Domain Admins group. The following message will appear: "The account <name> does not belong to the Domain Admins group. Do you want to continue?"

You may continue by clicking the **Yes** button. However keep in mind that in this case either the specified user must have full administrative access to all remotely running DeviceLock Services or DeviceLock Certificate (the public key) must be installed on every computer with DeviceLock Service.

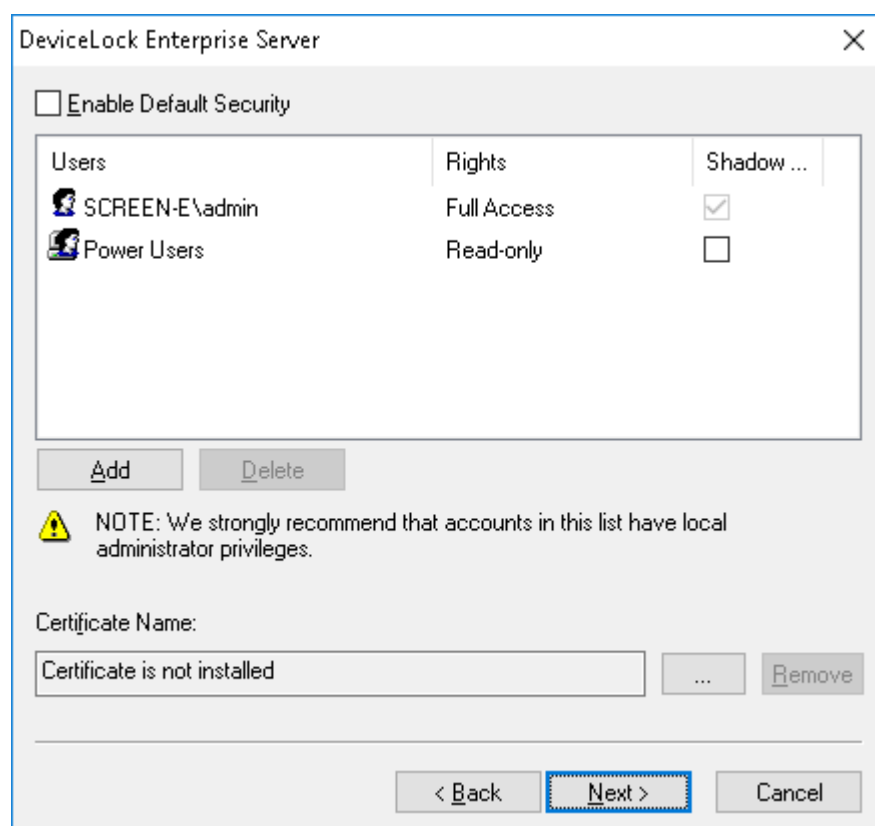
If the user's account specified for the **This account** option doesn't have the Log On As A Service system privilege, the wizard automatically assigns it. This privilege is needed to start the service on behalf of the user. The following message will appear: "The account <name> has been granted the Log On As A Service right."

If all of the service's startup parameters were specified correctly, the wizard starts DeviceLock Enterprise Server. The following message will appear: "Please wait while the program is interacting with a service. Starting service DLServer on Local Computer..."

It takes some time (up to a minute) before the DeviceLock Enterprise Server's service is started and the wizard's second page is displayed.

## Server administrators and certificate

On the second page, you can define the list of users that have administrative access to DeviceLock Enterprise Server and install DeviceLock Certificate (the private key).



### ***Enable Default Security***

In the default security configuration all users with local administrator privileges (i.e. members of the local Administrators group) can connect to DeviceLock Enterprise Server using a management console and change its setting and run reports.

To turn on the default security, select the **Enable Default Security** check box.

If you need to define more granular access to DeviceLock Enterprise Server, turn off the default security by clearing the **Enable Default Security** check box.

Then you need to specify authorized accounts (users and/or groups) that can connect to DeviceLock Enterprise Server. To add a new user or user group to the list of accounts, click on the **Add** button. You can add multiple accounts at a time.

To remove a record from the list of accounts, use the **Delete** button. By pressing and holding down the Ctrl or Shift key, you can select and remove multiple records at a time.

To determine the actions allowed to a user or group, select the desired level of access to the server:

- **Full access** - Allows the user or group to install and uninstall DeviceLock Enterprise Server, connect to it by using DeviceLock Management Console, and perform any actions on the server, such as making changes to server settings, creating, editing and running monitoring tasks and report creation tasks, viewing reports, and configuring policies.
- **Change** - Same as full access to the server with the exception of the right to make changes to the list of server administrators or change the level of access to the server for the users or groups already in that list.
- **Read-only** - Allows the user or group to connect to DeviceLock Enterprise Server by using DeviceLock Management Console, view server settings, run report creation tasks and view reports. This option does not give the right to make any changes on the server, create, edit or run monitoring tasks, create or edit report creation tasks, or configure policies.

For users and groups with **Change** or **Read-only** access, the **Shadow Data Access** option can be selected to allow access to shadow copies and user activity records. The users and groups with this option selected are allowed to open, view, and save shadow copies and user activity records from DeviceLock Enterprise Server logs by using Shadow Log Viewer (see [Shadow Log Viewer \(Server\)](#)) and UAM Log Viewer (see [Viewing User Activity](#)).

Without access to shadow data, DeviceLock Enterprise Server administrators do not have access to the content of shadow copies and user activity records. They cannot open, view, or save shadow copies and records of user activity.

---

### **Important**

We strongly recommend that DeviceLock Enterprise Server administrators be given local administrator rights as installing, updating, and uninstalling DeviceLock Enterprise Server may require access to Windows Service Control Manager (SCM) and shared network resources.

---

### ***Certificate Name***

You may need to deploy the private key to DeviceLock Enterprise Server if you want to enable authentication based on DeviceLock Certificate.

There are two methods of DeviceLock Enterprise Server authentication on remotely running DeviceLock Services:

- **User authentication** - The DeviceLock Enterprise Server service is running under the user's account that has full administrative access to DeviceLock Service on the remote computer. For more information on how to run DeviceLock Enterprise Server on behalf of the user, see the [Log on as](#) parameter description.
- **DeviceLock Certificate authentication** - In the situations where the user under which the DeviceLock Enterprise Server service is running can't access DeviceLock Service on the remote computer, you must authenticate based on a DeviceLock Certificate.  
*The public key should be installed on DeviceLock Service and the corresponding private key on DeviceLock Enterprise Server.*

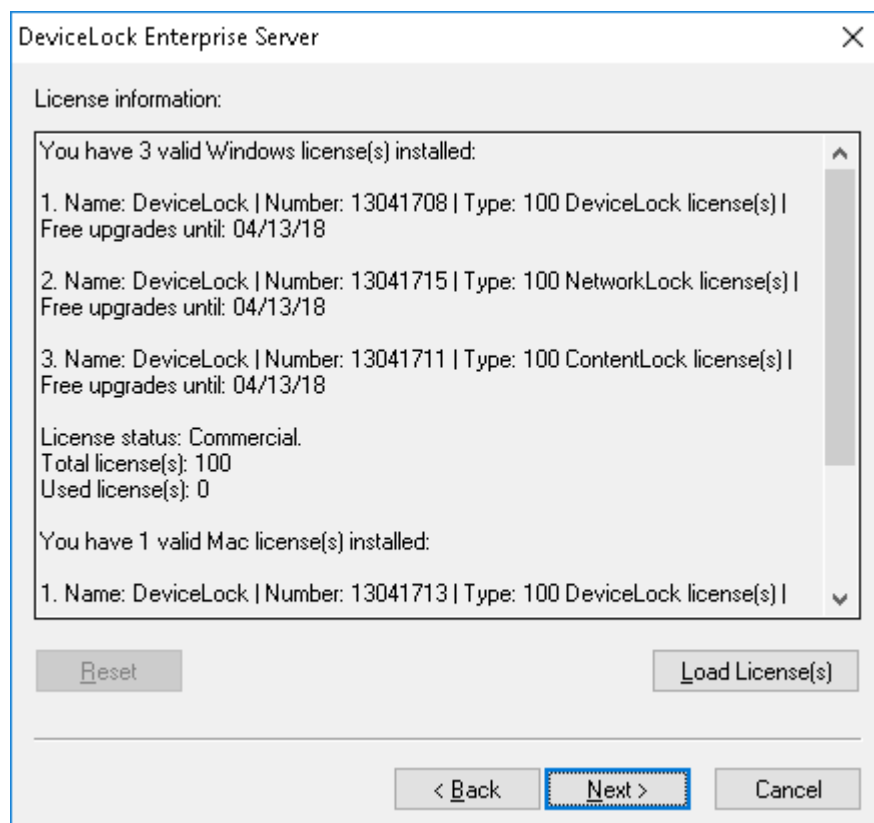
To install DeviceLock Certificate, click the  button, and select the file with a private key. To remove DeviceLock Certificate, click the **Remove** button.

For more information regarding DeviceLock Certificate, see the [DeviceLock Certificates](#) section later in this document.

Click the **Next** button to apply changes and proceed to the third page of the configuration wizard.

## License information

On this page, you can load your DeviceLock licenses.



If you've purchased a license for DeviceLock, you should load this license into DeviceLock Enterprise Server.

DeviceLock Enterprise Server handles only the licensed number of DeviceLock Services. For example, if you have a license for 100 computers but there are 101 DeviceLock Services working in your network, DeviceLock Enterprise Server will work with only first 100 DeviceLock Services and ignore the remaining one.

To load the license, click the **Load License(s)** button and select the license file.

You can load several license files in series - one by one.

After you have successfully loaded your license files, you can view the license information summary where **Total license(s)** displays the total number of purchased licenses while **Used license(s)** displays the number of licenses currently in use for collection of audit, shadowing and monitoring data on DeviceLock Enterprise Server.

If there are no valid licenses loaded, DeviceLock Enterprise Server works in the trial mode and can handle only two DeviceLock Services.

---

**Note**

If a computer with DeviceLock Service leaves the network, DeviceLock Enterprise Server will handle its replacement only after a restart or after 6 hours.

---

Click the **Next** button to install licenses and proceed to the fourth page.

## Database settings

On this page, the wizard prompts you to configure database parameters.

### Database name

In the **Database name** box, view or change the name of the database for DeviceLock Enterprise Server. The default name suggested by the wizard is **DeviceLockDB**.

---

### Note

You should not create a database with the specified name manually because the configuration wizard creates the database automatically or uses the existing one.

---

### Connection type

In the **Connection type** list, you can choose from the following database connection options:

- **SQL Server ODBC Driver** - Connect to Microsoft SQL Server by using an ODBC driver.  
The **Server name** parameter must contain the name of the computer running SQL Server along with the name of the SQL Server instance. A SQL Server name normally consists of two parts: the computer name and the instance name divided by a backslash (such as computer\instance). If the instance name is empty (default instance), the computer name is used as the SQL Server name. To retrieve SQL Server names available on your local network, click the **Browse** button. (You should have access to the remote registry of the SQL Server computer to retrieve the instance name.)  
If the **Server name** parameter is empty, it means that SQL Server runs on the same computer as DeviceLock Enterprise Server and has the empty (default) instance name.  
To connect to SQL Server, authentication parameters must be configured as well.

Select the **Windows authentication** option to authenticate on SQL Server under the account used to run the DeviceLock Enterprise Server's service.

If the service runs under the SYSTEM account, and SQL Server is on a remote computer, the service will not be able to connect to SQL Server since the SYSTEM account does not have the right to access the network. For more information on how to run DeviceLock Enterprise Server on behalf of a user, see the [Log on as](#) parameter description.

Select the **SQL Server authentication** option to allow SQL Server to perform authentication by checking the login and password previously defined. Before selecting the **SQL Server authentication** option, make sure that your SQL Server is configured for mixed-mode authentication. Enter the SQL Server user name (login) in **Login name** and its password in **Password**.

---

**Note**

Windows Authentication is more secure than SQL Server Authentication. When possible, you should use Windows Authentication.

---

- **PostgreSQL ODBC Driver** - Connect to the PostgreSQL server by using an ODBC driver. This option requires PostgreSQL ODBC Driver version 9.6.500 or later. You can download this driver from the PostgreSQL website at [postgresql.org/ftp/odbc/versions/msi](https://postgresql.org/ftp/odbc/versions/msi).

The **Server name** parameter specifies the name of the computer running PostgreSQL. If this parameter is empty, then PostgreSQL is deemed to run on the same computer as DeviceLock Enterprise Server.

The **Login name** parameter specifies the name of the PostgreSQL user, and the **Password** field is used to enter the password of that user. The configuration wizard uses this login to create or update the database, so one should choose a user with sufficient access rights. This login is also used for read/write access to the database during DeviceLock Enterprise Server operation.

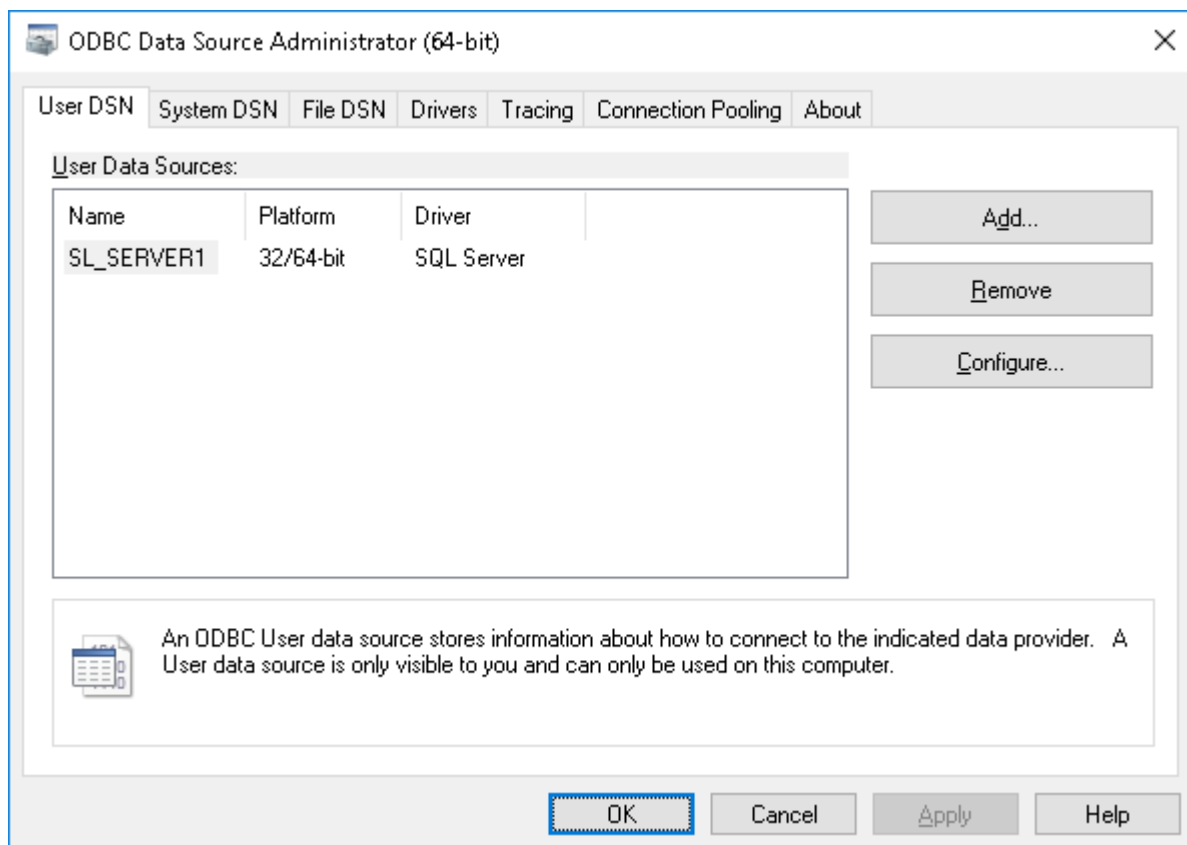
---

**Note**

If the ODBC Driver for PostgreSQL Server is not installed or is outdated, you can install DeviceLock Enterprise Server without configuring the database. In this case, you should install the required ODBC Driver later, and then configure the database using the DeviceLock Management Console (see [Administering DeviceLock Enterprise Server](#)).

---

- **System Data Source** - Connect to the database server by using a previously created system data source. Select a data source from the **Data source name** list.  
To create a data source, use **ODBC Data Source Administrator** from **Control Panel > Administrative Tools**.



If the data source requires a login name and password (such as when using SQL Server Authentication or connecting to PostgreSQL), then you need to specify the appropriate name and password in the **Login name** and **Password** fields. Otherwise, leave these fields blank.

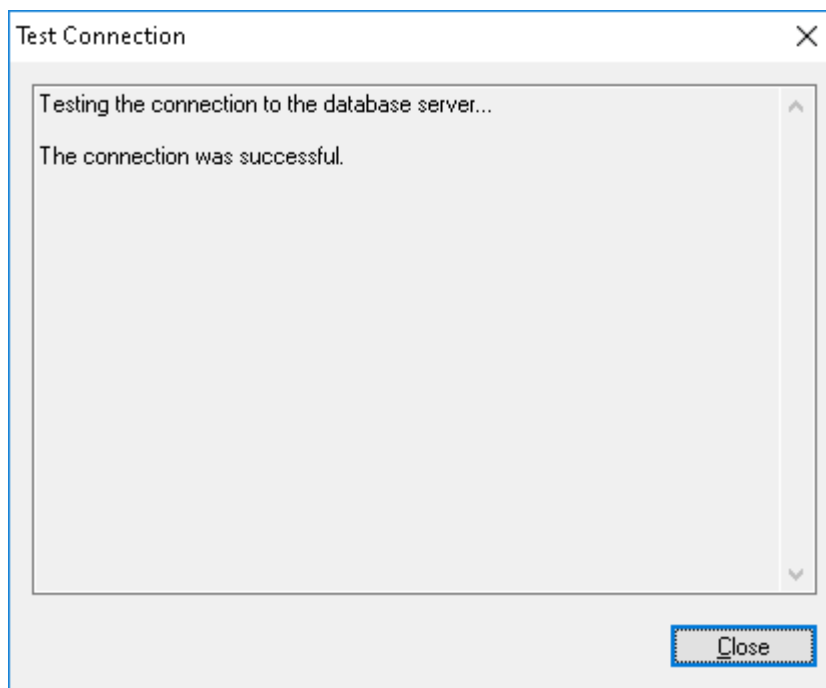
To refresh the **Data Source Name** list, click the **Refresh** button.

## Test Connection

Having specified the connection parameters, you could verify them to make sure they are correct. Click the **Test Connection** button to begin.

Please note that it only checks connectivity to the database server. In case of problems with access to the database while successfully connected to the database server, you won't see those problems in the **Test Connection** dialog box.





If some connection parameters were specified incorrectly, you may see one of these errors:

- **SQL Server does not exist or access denied** - An incorrect SQL Server name is specified in the **Server name** parameter or the remote SQL Server's computer is not accessible. It is possible that you've specified the name of the computer running SQL Server but this SQL Server also has an instance name which should be specified as well (e.g. computer\instance).
- **Login failed for user 'COMPUTER\_NAME\$'** - Windows Authentication is selected but the user account used to run the DeviceLock Enterprise Server service can't get access to the computer with SQL Server. It may happen when the service starts either under the SYSTEM user or on behalf of a user that doesn't have local administrative privileges on the remote SQL Server's computer.
- **Login failed for user 'user\_name'** - SQL Server Authentication is selected and an incorrect SQL user name (login) or password is supplied. Please note that SQL users are different from Windows users and you can't use the regular Windows account in the **Login name** parameter. SQL users exist only in SQL Server and to manage them you should use SQL Server management consoles (such as Microsoft SQL Server Management Studio).
- **Login failed for user 'user\_name'. The user is not associated with a trusted SQL Server connection** - SQL Server Authentication is selected but your SQL Server doesn't support this mode. You should either use Windows Authentication or allow your SQL Server to work in the mixed mode (SQL Server and Windows Authentication mode).
- **Login failed for user ''**. **The user is not associated with a trusted SQL Server connection** - The data source specified in **Data Source Name** is configured to use the SQL Server Authentication mode but the **Login name** parameter is empty.
- **Data source name not found and no default driver specified** - You've selected **System Data Source** from the **Connection type** list and specified either an empty or non-existent name in **Data Source Name**.

## Store shadow files in the database

Shadow data can be stored in the server's database or it can be stored in files on the disk. To store it in the database, select the **Store shadow files in the database** check box.

If storing shadow data in the database on the Microsoft SQL Server, it is advisable to substantially increase the maximum file size parameter for the transaction log of the database. Otherwise, SQL Server may fail to handle large amounts of data in one transaction. For best results, use a 64-bit SQL Server edition, and increase the amount of memory available to SQL Server. On a 32-bit computer, enable AWE (Address Windowing Extensions). For instructions, see Microsoft's article at [technet.microsoft.com/library/ms190673\(v=sql.90\).aspx](https://technet.microsoft.com/library/ms190673(v=sql.90).aspx).

To store data on the disk, clear the **Store shadow files in the database** check box. In this case only links to the binary data and some additional information are stored in the server's database.

When stored on the disk, data files are located by the path specified in the **Store path** parameter. To choose the folder where files should be stored, you can use the **Browse** button.

You can also specify the network shared resource (e.g. \\server\d1store) that will be used as storage. Make sure that the user account used to run the DeviceLock Enterprise Server service has full access to this network resource.

---

### Note

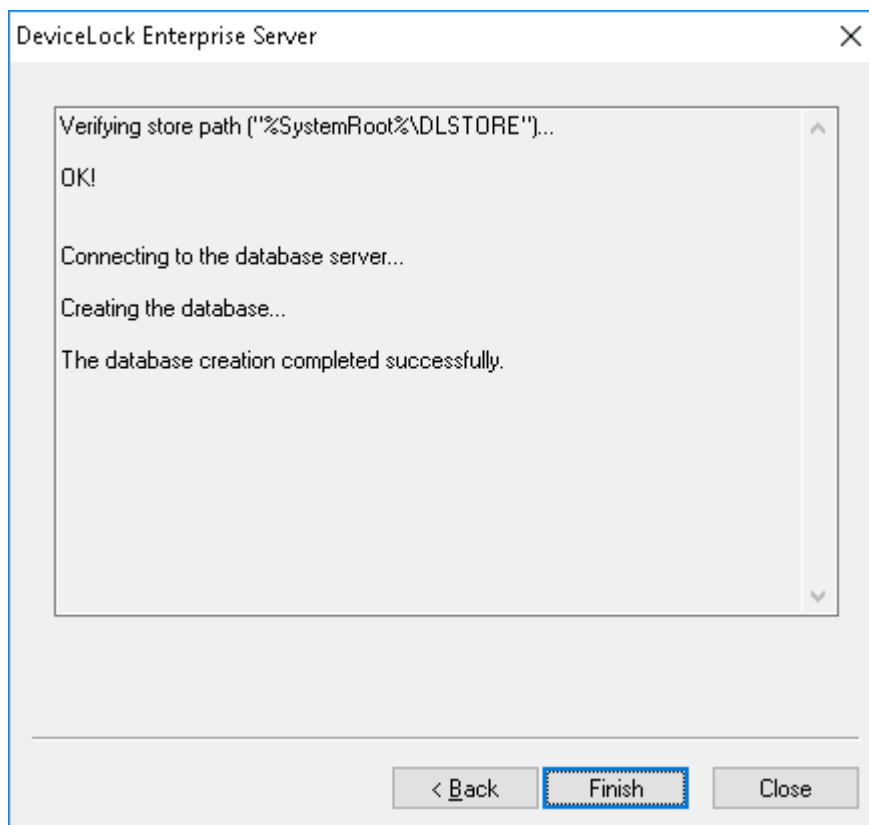
We recommend storing binary data on the disk.

---

Click the **Next** button to apply changes and proceed to the last page.

## Completing configuration

It takes some time to create the database specified in **Database name** if it does not exist on this database server yet. If the database already exists and it has the proper format (i.e. it was created by DeviceLock) then DeviceLock Enterprise Server keeps all existing data and uses this database. If necessary, DeviceLock automatically updates the database to the latest version.



On this page of the configuration wizard you can observe the applying of the database settings specified, and view errors that might occur when configuring the database.

If some parameters on the previous page of the wizard were specified incorrectly, you might encounter the following errors:

- **[2] The system cannot find the file specified** - The DeviceLock Enterprise Server is set to store binary data on the disk but the path specified in **Store path** is incorrect. If you've specified the shared network resource then it is possible that this network resource is not accessible.
- **Failed to verify store path. [5] Access is denied** - The path specified in the **Store path** parameter is correct, but the user account used to run the DeviceLock Enterprise Server service doesn't have full access to files by this path.
- **CREATE DATABASE permission denied in database 'name'** - The user account (login) used to connect to SQL Server doesn't have sufficient rights to create the database. The login should have at least the dbcreator Server role (see **Server Roles** in **Login Properties** of Microsoft SQL Server Management Studio).
- **The server principal "user\_name" is not able to access the database "name" under the current security context** - The user account (login) used to connect to SQL Server doesn't have access to the existing database. The login should be mapped to this database (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** - The user account (login) used to connect to SQL Server doesn't have read/write access to the existing

database. The login should have at least db\_datareader and db\_datawriter Database roles (see **User Mapping in Login Properties** of Microsoft SQL Server Management Studio).

- **Invalid object name 'name'** - The database specified in the **Database name** parameter already exists in this SQL Server but has an incorrect format. It happens when you are trying to use the database that was not created by DeviceLock Enterprise Server or if the database was corrupted.
- **DeviceLock Database has an unsupported format** - The database specified in the **Database name** parameter already exists but is outdated. This existing database has an unsupported format so it can't be automatically upgraded to the new format. You should either use another database or create a new one.
- **DeviceLock Database has a format that is not supported by the current server version** - The database specified in the **Database name** parameter already exists but it was created by the more recent version of DeviceLock Enterprise Server. You should either use the latest version of DeviceLock Enterprise Server or use another database (or create a new one).

The wizard might also display some of the SQL Server connection errors listed in the [Test Connection](#) section earlier in this document.

Use the **Back** button to return to the previous page of the wizard and make necessary changes.

If there are no errors, click the **Finish** button to close the configuration wizard and continue the installation process.

Then, on the **Installation Wizard Completed** page, click **Finish** to complete the installation. On this page, you will have the option to go to the DeviceLock home page. This option is selected by default.

---

#### Note

You can uninstall DeviceLock as follows:

- Use **Programs and Features** in Control Panel (**Add or Remove Programs** on earlier versions of Windows) to remove **DeviceLock**.  
- OR -
  - Select **Remove DeviceLock** on the Windows **Start** menu.
- 

## Installing DeviceLock Content Security Server

This section covers the steps to install DeviceLock Content Security Server:

1. [Prepare to Install](#)
2. [Start Installation](#)
3. [Perform Configuration and Complete Installation](#)

### Prepare to Install

Before you install DeviceLock Content Security Server, consider the following:

- The DeviceLock Content Security Server setup program installs two DeviceLock components: Search Server and Discovery Server.

- To install and operate DeviceLock Content Security Server, the following system requirements must be met:

<b>Operating system</b>	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, or Windows Server 2019.  Installation is supported on both 32-bit and 64-bit operating systems.
<b>Database server</b>	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017, or 2019, any edition, including SQL Server Express.  <b>Important</b> Database server is required to run the Search Server and Discovery Server (see <a href="#">Database settings</a> for details).
<b>Hard disk space</b>	Minimum: 1 GB  Recommended: 800 GB (in case of local database server)

- You must have administrator permissions to install DeviceLock Content Security Server.
- For optimal performance and reliability, we recommend that you install DeviceLock Enterprise Server and DeviceLock Content Security Server on different computers.
- There is a special Search Server license which you must purchase for DeviceLock Content Security Server. You can use the same license on an unlimited number of computers running DeviceLock Content Security Server.  
Search Server licensing is based on the number of log entries to be indexed for full-text search. Each license allows the indexing of 1,000 entries in the Shadow Log (including shadow copies), 1,000 entries in the UAM log (including keyboard input records), and 5,000 entries in each of the other logs (Audit Log, Deleted Shadow Data Log, Server Log, Monitoring Log, and Policy Log). Depending upon the actual number of log entries on your DeviceLock Enterprise Server/s, you can purchase as many licenses as required. If using several licenses, the Search Server can index as many log entries as the total license count allows. Additional Search Server licenses can be purchased and installed at any time.  
The trial period for DeviceLock Content Security Server is 30 days. During the trial period, the Search Server can index 2,000 entries in the Shadow Log, 2,000 entries in the UAM Log, and 10,000 entries in each of the other logs.
- There is a special DeviceLock Discovery license which you must purchase for DeviceLock Content Security Server. A license is required for each computer or network resource scanned with DeviceLock Discovery, regardless of whether you are going to scan the entire computer or a single folder. The trial period for DeviceLock Discovery is 30 days. During this period, DeviceLock Discovery can scan no more than two computers or network resources.
- In case you have several DeviceLock Enterprise Servers on your network, you can also install several DeviceLock Content Security Servers to balance the load.
- When several DeviceLock Content Security Servers are deployed, each Search Server has its own search index. Hence, you have to connect to every DeviceLock Content Security Server and run

the same search queries on every Search Server in order to get the complete result set from all the data stored on all DeviceLock Enterprise Servers.

- There are two options for connecting DeviceLock Content Security Server and the database server. Before installing DeviceLock Content Security Server, decide which option best suits your needs:
  1. ONE-TO-ONE - Installing one DeviceLock Content Security Server and connecting it to one database server. This option is most appropriate for small networks (up to several hundred computers).
  2. MANY-TO-MANY - Installing several DeviceLock Content Security Servers and connecting each to its own database server. This option is typical for medium and large networks geographically distributed across a variety of segments.
- We strongly recommend that you exit all Windows programs before you start Setup.

## Start Installation

Use this procedure to begin the installation process.

### ***To start installation***

1. Open the archive DeviceLock.zip, and then double-click the file setup\_dlcss.exe to start the Setup program.  
*You must run the Setup program on each computer on which you want to install DeviceLock Content Security Server.*
2. Follow the instructions in the Setup program.
3. On the **License Agreement** page, read the License Agreement and then click **I accept the terms in the license agreement** to accept the licensing terms and conditions and proceed with the installation.
4. On the **Customer Information** page, type your user name and organization, and then click **Next**.
5. On the **Destination Folder** page, accept the default installation folder or click **Change** to modify the path as needed. Click **Next**.  
The default installation folder is %ProgramFiles%\DeviceLock Content Security Server on 32-bit Windows or %ProgramFiles(x86)%\DeviceLock Content Security Server on 64-bit Windows.
6. On the **Ready to Install the Program** page, click **Install** to begin the installation.  
*The DeviceLock Content Security Server configuration wizard starts.*  
If you are installing an upgrade or simply reinstalling DeviceLock Content Security Server, and want to keep its current configuration, you do not need to go through the configuration wizard again - just click **Next** and then **Cancel** to close the wizard and keep all existing settings unchanged.  
In case you need to change some parameters but keep others - edit only needed parameters and go through all the configuration wizard's pages up to the **Finish** button on the final page.

### Note

If you are installing Content Security Server for the first time (there are no existing settings on this computer yet) and you cancel the configuration wizard, Setup will not be able to install DeviceLock Content Security Server's service, so you will need to run the configuration wizard again.

## Perform Configuration and Complete Installation

The configuration wizard opens automatically during the installation process. This wizard provides the following pages to configure DeviceLock Content Security Server:

- [Service account and connection settings](#)
- [Server administrators and certificate](#)
- [License information](#)
- [Database settings](#)
- [Completing configuration](#)

### Service account and connection settings

On this page, you configure startup options for the DeviceLock Content Security Server service.

The screenshot shows the 'DeviceLock Content Security Server' configuration window. It has two main sections: 'Log on as' and 'Connection settings'. In the 'Log on as' section, the 'Local System account' radio button is unselected, and the 'This account:' radio button is selected. The text box next to 'This account:' contains 'SCREEN-E\admin'. To the right of this text box is a 'Browse...' button. Below the 'This account:' text box are two password fields: 'Password:' and 'Confirm password:', both containing masked characters (dots). In the 'Connection settings' section, the 'Dynamic ports' radio button is selected, and the 'Fixed TCP port:' radio button is unselected. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

### Log on as

First of all, you should choose an account under which the DeviceLock Content Security Server service will start. As with many other Windows services, the DeviceLock Content Security Server service can start under the special local system account (the SYSTEM user) and on behalf of any user.

To start the service under the SYSTEM user, select the **Local System account** option. Keep in mind that the process working under the SYSTEM user cannot access shared network resources and authenticates on remote computers as an anonymous user. Therefore, DeviceLock Content Security Server configured to run under the SYSTEM user is not able to access DeviceLock Enterprise Server running on the remote computer and it must use DeviceLock Certificate for authentication on it.

For more information about authentication methods, see description of the [Certificate Name](#) parameter.

---

### Important

If the DeviceLock Content Security Server service is configured to run under the Local System account, DeviceLock Discovery Server cannot install or remove DeviceLock Discovery Agents on remote computers.

---

To start the service on behalf of the user, select the **This account** option, enter the user's account name and the password. It is recommended to use a user account that has administrative privileges on all the computers where DeviceLock Enterprise Server is running. Otherwise, you will need to use DeviceLock Certificate authentication.

If you are installing DeviceLock Content Security Server in the domain environment, we recommend that you use a user account that is a member of the Domain Admins group. Since Domain Admins is a member of the local group Administrators on every computer in the domain, members of Domain Admins will have full access to every computer.

Also, consider the following:

- If **Default Security** is disabled on a remote DeviceLock Enterprise Server, the user account specified in the **This account** option must be also in the list of server administrators with at least **Read-only** level of access on that DeviceLock Enterprise Server. Otherwise, the DeviceLock Certificate authentication needs to be used.
- If **Default Security** is disabled on a remote DeviceLock Service, the user account specified in the **This account** option must be also in the list of DeviceLock administrators with at least **Read-only** access rights on that DeviceLock Service. Otherwise, the DeviceLock Certificate authentication should be used or explicit credentials should be specified in the respective DeviceLock Discovery unit.

### Connection settings

You can instruct DeviceLock Content Security Server to use a fixed TCP port for communication with the management console, making it easier to configure a firewall. Type the port number in **Fixed TCP port**. To use dynamic ports for RPC communication, select the **Dynamic ports** option. By default, DeviceLock Content Security Server uses port 9134.



Click **Next** to start the DeviceLock Content Security Server service and to proceed to the second page.

## Starting the Service

If the current user does not have full administrative access to DeviceLock Content Security Server (in case it already exists and you're installing an upgrade), the configuration wizard will not be able to install the service and apply changes. The following message will appear: "Access is denied." Also, a similar error may occur when the current user does not have local administrative privileges on the computer where DeviceLock Content Security Server is installing.

If you have specified an incorrect user name for the **This account** option or the wrong user password, DeviceLock Content Security Server will not be able to start. The following message will appear: "The account name is invalid or does not exist, or the password is invalid for the account name specified."

You will be notified if the user's account specified for the **This account** option is not a member of the Domain Admins group. The following message will appear: "The account <name> does not belong to the Domain Admins group. Do you want to continue?"

You may continue by clicking **Yes**. However, make sure that either of the following is true.

For Search Server:

- The specified user has administrative access to all remotely running DeviceLock Enterprise Servers
- OR -
- DeviceLock Certificate (private key) is installed on every computer running DeviceLock Enterprise Server

For DeviceLock Discovery Server:

- The specified user has administrative access to all computers scanned by DeviceLock Discovery Server. This includes computers running DeviceLock Services, DeviceLock Discovery Agents, as well as any computers not having the Agent installed.
- OR -
- DeviceLock Certificate (public key) is installed on every computer (with DeviceLock Service) scanned by DeviceLock Discovery Server
- OR -
- Credentials for accessing remote computers are specified in the scanning settings.

If the user's account specified for the **This account** option does not have the "Log On As A Service" system privilege, the wizard automatically assigns it. This privilege is needed to start the service on behalf of the user. The following message will appear: "The account <name> has been granted the Log On As A Service right."

If all of the service's startup parameters were specified correctly, the wizard starts DeviceLock Content Security Server. The following message will appear: "Please wait while the program is interacting with a service. Starting service DLCSS on Local Computer..."

It takes some time (up to a minute) before the DeviceLock Content Security Server service is started and the next page of the wizard is displayed.

## Server administrators and certificate

On this page of the wizard, you can set up the list of users that have administrative access to DeviceLock Content Security Server, and install DeviceLock Certificate (the private key) if needed.

The screenshot shows the 'DeviceLock Content Security Server' configuration window. At the top, there is a checkbox labeled 'Enable Default Security' which is checked. Below this is a table with three columns: 'Users', 'Rights', and 'Shadow ...'. The table is currently empty. Below the table are two buttons: 'Add' and 'Delete'. A note with a triangle icon states: 'NOTE: We strongly recommend that accounts in this list have local administrator privileges.' Below the note is a section for 'Certificate Name:' with a text box containing 'Certificate is not installed', a button with three dots, and a 'Remove' button. At the bottom of the window are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

### **Enable Default Security**

In the default security configuration all users with local administrator privileges (i.e. members of the local Administrators group) can connect to DeviceLock Content Security Server using a management console, change its settings, run search queries, configure content detection settings, and run discovery tasks.

To turn on the default security, select the **Enable Default Security** check box.

If you need to define more granular access to DeviceLock Content Security Server, turn off the default security by clearing the **Enable Default Security** check box.

Then you need to specify authorized accounts (users and/or groups) that can connect to DeviceLock Content Security Server. To add a new user or group to the list of accounts, click **Add**. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using Ctrl and/or Shift you can highlight and remove several records simultaneously.

To determine the actions allowed to a user or group, select the desired level of access to the server:

- **Full access** - Allows the user or group to install and uninstall DeviceLock Content Security Server, connect to it by using DeviceLock Management Console, and perform any actions on the server, such as: view and change server settings; create and run search queries and tasks; view and change content detection settings; create and run discovery tasks and reports.
- **Change** - Same as full access to the server with the exception of the right to make changes to the list of server administrators or change the level of access to the server for the users or groups already in that list.
- **Read-only** - Allows the user or group to connect to DeviceLock Content Security Server by using DeviceLock Management Console; view server settings; run search queries; view and run existing search tasks; view content detection settings; view discovery reports and manually create new reports based on the existing reports and data already prepared by discovery tasks. This option does not give the right to run discovery tasks, make any changes on the server, or create a new index for the Search Server.

For users and groups with **Change** or **Read-only** access, the **Shadow Data Access** option can be selected to allow access to shadow copies and user activity records. The users and groups with this option selected are allowed to search the content of shadow copies and user activity records, and open, view, and save shadow copies and user activity records from search results.

Without access to shadow data, DeviceLock Content Security Server administrators cannot open, view, or save shadow copies and records of user activity. Search results do not have the **Open**, **Save**, and **View** links, and asterisks are displayed instead of text snippets of shadow copies and user activity records. Logins and passwords in document parameters for user activity records are also replaced with asterisks.

---

### Important

We strongly recommend that DeviceLock Content Security Server administrators be given local administrator rights as installing, updating and uninstalling this server may require access to Windows Service Control Manager (SCM) and shared network resources.

---

### Certificate Name

You may need to deploy the private key to DeviceLock Content Security Server if you want to enable authentication based on DeviceLock Certificate.


There are two methods of DeviceLock Search Server authentication on a remotely running DeviceLock Enterprise Server:

- **User authentication** - The DeviceLock Content Security Server service is running under the user's account that has administrative access to DeviceLock Enterprise Server on the remote computer. For more information on how to run DeviceLock Content Security Server on behalf of the user, please read the description of the [Log on as](#) parameter.
- **DeviceLock Certificate authentication** - In situations where the user under which the DeviceLock Content Security Server service is running cannot access DeviceLock Enterprise Server on the remote computer, you must authenticate based on a DeviceLock Certificate.

*The same private key should be installed on DeviceLock Enterprise Server and on DeviceLock Content Security Server.*

There are three methods of DeviceLock Discovery Server authentication when scanning a remote computer:

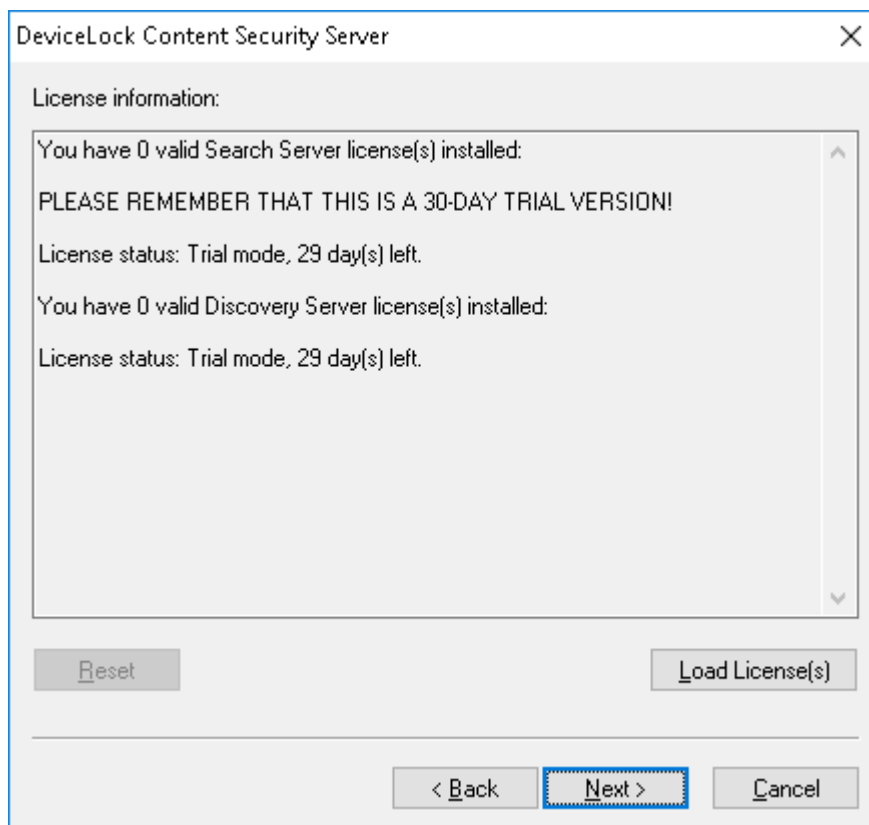
- **User authentication** - The DeviceLock Content Security Server service is running under a certain user account, and these credentials are used to access remote computers being scanned. These credentials will be supplied to either DeviceLock Service, DeviceLock Discovery Agent, or the remote computer if scanning is performed without an agent. For more information on how to run DeviceLock Content Security Server on behalf of a user, please read the description of the [Log on as](#) parameter.
- **Alternative credentials authentication** - The DeviceLock Content Security Server service is running under a user account that has administrative privileges at least on the local computer. DeviceLock Discovery Server will use alternative credentials to log in to remote computer being scanned.
- **DeviceLock Certificate authentication** - Authentication based on a DeviceLock Certificate is used to authenticate on remote computers running DeviceLock Service with the certificate's public key installed.

To install DeviceLock Certificate, click the  button, and select the file containing the certificate's private key. To remove DeviceLock Certificate, click **Remove**.

Click **Next** to apply changes and proceed to the next page of the configuration wizard.

## License information

On this page, you can install your licenses for Search Server and/or DeviceLock Discovery. Search Server and DeviceLock Discovery are licensed separately. The trial period is 30 days.



To install a license, click **Load License(s)** and select the license file. You can load several license files in series - one by one. The **License information** box displays summary information about the licenses you're installing.

After Content Security Server has been installed, you can use the DeviceLock Management Console to install a license or view the current license information, including the number of installed licenses and the number of used licenses for Search Server and/or DeviceLock Discovery.

Click **Next** to proceed to configuring the database.

## Database settings

On this page, the wizard prompts you to configure database parameters.

### Important

Do not skip this page, as a database is required for the Search Server and Discovery Server to function. Without a database, it is impossible to search using content-aware groups, save and automate search queries, or use the Discovery Server for content discovery.

### Database name

In the **Database name** box, view or change the name of the database for DeviceLock Content Security Server. The default name suggested by the wizard is **DLCSSDB**.

### Note

You should not create a database with the specified name manually because the configuration wizard creates the database automatically or uses the existing one.

### Connection type

In the **Connection type** list, you can choose from the following database connection options:

- **SQL Server ODBC Driver** - Connect to Microsoft SQL Server by using an ODBC driver. The **SQL Server name** parameter must contain the name of the computer running SQL Server along with the name of the SQL Server instance. A SQL Server name normally consists of two parts: the computer name and the instance name divided by a backslash (such as computer\instance). If the instance name is empty (default instance), the computer name is used as the SQL Server name. To retrieve SQL Server names available on your local network, click the

**Browse** button. (You should have access to the remote registry of the SQL Server computer to retrieve the instance name.)

If the **SQL Server name** parameter is empty, it means that SQL Server runs on the same computer as DeviceLock Content Security Server and has the empty (default) instance name.

To connect to SQL Server, authentication parameters must be configured as well.

Select the **Windows authentication** option to authenticate on SQL Server under the account used to run the DeviceLock Content Security Server's service.

If the service runs under the SYSTEM account and SQL Server is on a remote computer, the service will not be able to connect to SQL Server since the SYSTEM account doesn't have the right to access the network. For more information on how to run DeviceLock Content Security Server on behalf of a user, see the description of the [Log on as](#) parameter.

Select the **SQL Server authentication** option to allow SQL Server to perform authentication by checking the login and password previously defined. Before selecting the **SQL Server authentication** option, make sure that your SQL Server is configured for mixed-mode authentication. Enter the SQL Server user name (login) in **Login name** and its password in **Password**.

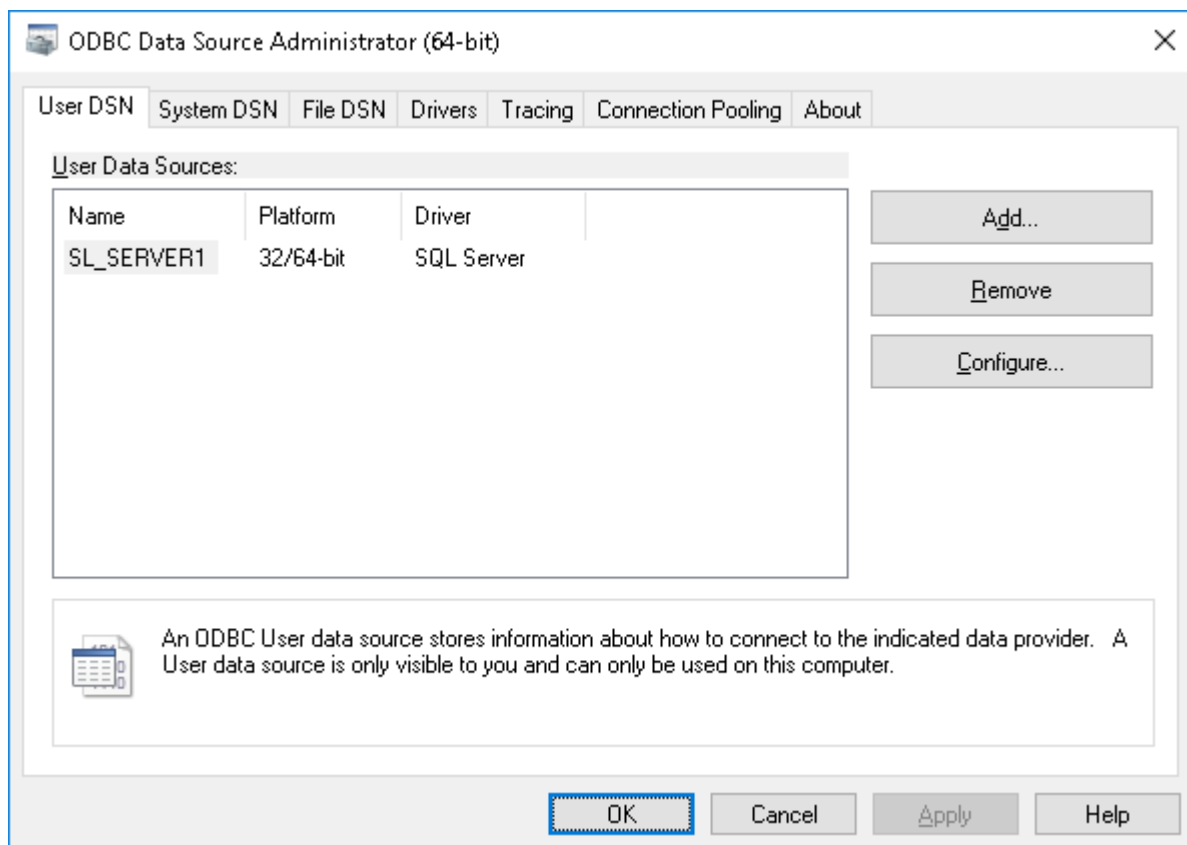
---

**Note**

Windows Authentication is more secure than SQL Server Authentication. When possible, you should use Windows Authentication.

---

- **System Data Source** - Connect to the database server by using a previously created system data source. Select a data source from the **Data Source Name** list.  
To create a data source, use **ODBC Data Source Administrator** from **Control Panel > Administrative Tools**.



If the data source requires a login name and password (such as when using SQL Server Authentication), then you need to specify the appropriate name and password in the **Login name** and **Password** fields. Otherwise, leave these fields blank.

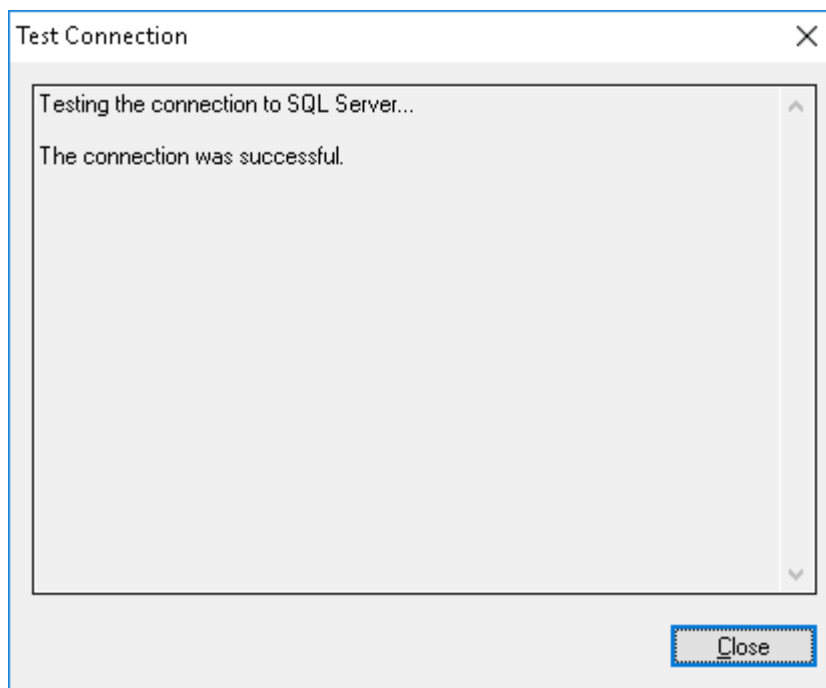
To refresh the **Data Source Name** list, click the **Refresh** button.

## Test Connection

Having specified the connection parameters, you could verify them to make sure they are correct. Click the **Test Connection** button to begin.

Please note that it only checks connectivity to the database server. In case of problems with access to the database while successfully connected to the database server, you won't see those problems in the **Test Connection** dialog box.





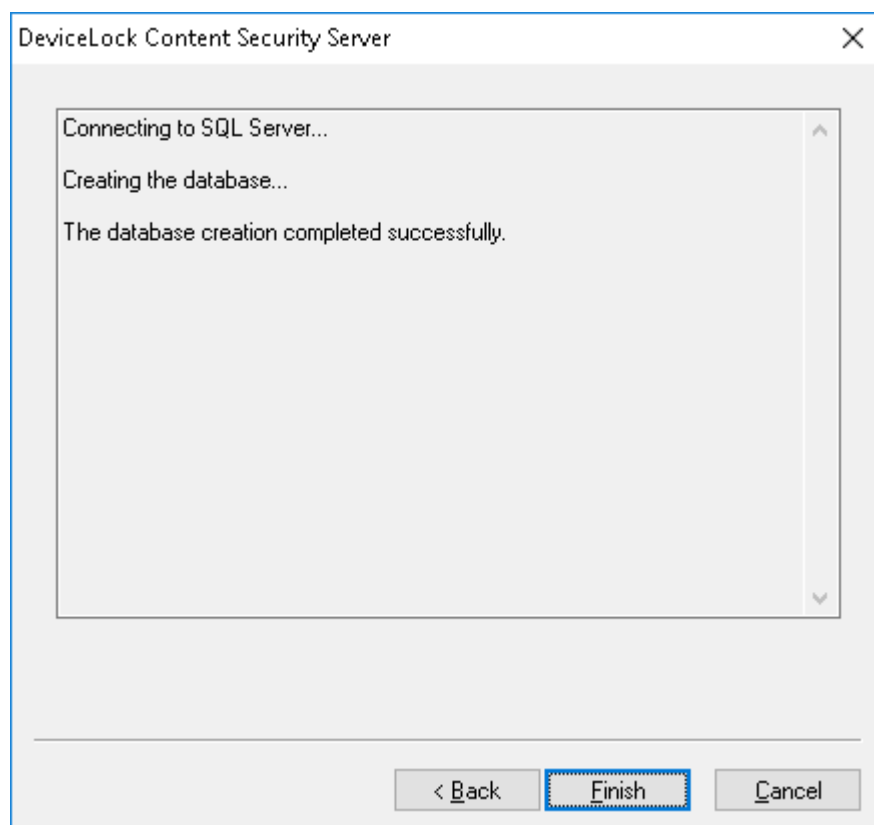
If some connection parameters were specified incorrectly, you may see one of these errors:

- **SQL Server does not exist or access denied** - An incorrect SQL Server name is specified in the **SQL Server name** parameter or the remote SQL Server's computer is not accessible. It is possible that you've specified the name of the computer running SQL Server but this SQL Server also has an instance name which should be specified as well (e.g. computer\instance).
- **Login failed for user 'COMPUTER\_NAME\$'** - Windows Authentication is selected but the user account used to run the DeviceLock Content Security Server service can't get access to the computer with SQL Server. It may happen when the service starts either under the SYSTEM user or on behalf of a user that doesn't have local administrative privileges on the remote SQL Server's computer.
- **Login failed for user 'user\_name'** - SQL Server Authentication is selected with either an incorrect SQL user name (login) or wrong password specified. Please note that SQL users are different from Windows users and you can't use the regular Windows account in the **Login name** parameter. SQL users exist only in SQL Server and to manage them you should use SQL Server management consoles (such as Microsoft SQL Server Management Studio).
- **Login failed for user 'user\_name'. The user is not associated with a trusted SQL Server connection** - SQL Server Authentication is but your SQL Server doesn't support this mode. You should either use Windows Authentication or allow your SQL Server to work in the mixed mode (SQL Server and Windows Authentication mode).
- **Login failed for user ''**. **The user is not associated with a trusted SQL Server connection** - The data source specified in **Data Source Name** is configured to use the SQL Server Authentication mode but the **Login name** parameter is empty.
- **Data source name not found and no default driver specified** - You've selected **System Data Source** from the **Connection type** list and specified either an empty or non-existent name in **Data Source Name**.

Click the **Next** button to apply changes and proceed to the last page.

## Completing configuration

It takes some time to create the database specified in **Database name** if it does not exist on this database server yet. If the database already exists and it has the proper format (i.e. was created by DeviceLock) then DeviceLock Content Security Server keeps all existing data and uses this database. If necessary, DeviceLock automatically updates the database to the latest version.



On this page of the configuration wizard you can observe the applying of the database settings specified, and view errors that might occur when configuring the database.

If some parameters on the previous page of the wizard were specified incorrectly, you might encounter the following errors:

- **CREATE DATABASE permission denied in database 'name'** - The user account (login) used to connect to SQL Server doesn't have sufficient rights to create the database. The login should have at least the dbcreator Server role (see **Server Roles** in **Login Properties** of Microsoft SQL Server Management Studio).
- **The server principal "user\_name" is not able to access the database "name" under the current security context** - The user account (login) used to connect to SQL Server doesn't have access to the existing database. The login should be mapped to this database (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** - The user account (login) used to connect to SQL Server doesn't have read/write access to the existing

database. The login should have at least db\_datareader and db\_datawriter Database roles (see **User Mapping in Login Properties** of Microsoft SQL Server Management Studio).

- **Invalid object name 'name'** - The database specified in the **Database name** parameter already exists on this SQL Server but has an incorrect format. It happens when you are trying to use the database that was not created by DeviceLock Content Security Server or if the database was corrupted.
- **DeviceLock Database has an unsupported format** - The database specified in the **Database name** parameter already exists but is outdated. This existing database has an unsupported format so it can't be automatically upgraded to the new format. You should either use another database or create a new one.
- **DeviceLock Database has a format that is not supported by the current server version** - The database specified in the **Database name** parameter already exists but it was created by the more recent version of DeviceLock Content Security Server. You should either use the latest version of DeviceLock Content Security Server or use another database (or create a new one).

Also, the wizard might display some of the SQL Server connection errors listed in the [Test Connection](#) section earlier in this document.

Use the **Back** button to return to the previous page of the wizard and make necessary changes.

If there are no errors, click the **Finish** button to close the wizard and continue the installation process.

Next, on the **Installation Wizard Completed** page, click **Finish** to complete the installation. On this page, you will have the option to go to the DeviceLock home page. This option is selected by default.

---

#### Note

You can uninstall DeviceLock Content Security Server as follows:

- Use **Programs and Features** in Control Panel (**Add or Remove Programs** on earlier versions of Windows) to remove **DeviceLock Content Security Server**,  
- OR -
  - Select **Remove DeviceLock Content Security Server** on the Windows **Start** menu.
-

# DeviceLock Consoles and Tools

## DeviceLock Management Console

DeviceLock Management Console is a snap-in for Microsoft Management Console (MMC).

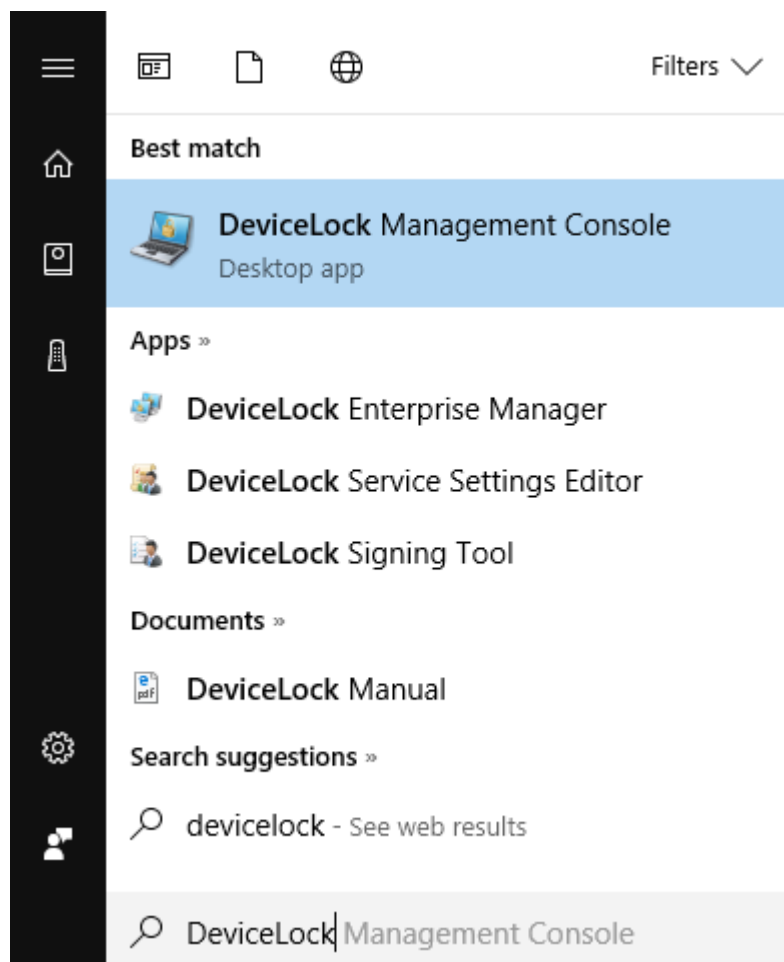
Using DeviceLock Management Console, you can view and change permissions and audit rules, install and update DeviceLock Service as well as view audit records for individual computers.

DeviceLock Management Console is also used to view logs stored on DeviceLock Enterprise Server, running search queries on DeviceLock Content Security Server and for managing these servers.

DeviceLock Management Console should be used on the computer from which the administrator is managing DeviceLock Services, DeviceLock Enterprise Servers and DeviceLock Content Security Servers on the network.

For information on how to install DeviceLock Management Console, see [Installing Management Consoles](#).

You can open the console by running the DeviceLock Management Console app from the Windows start page.

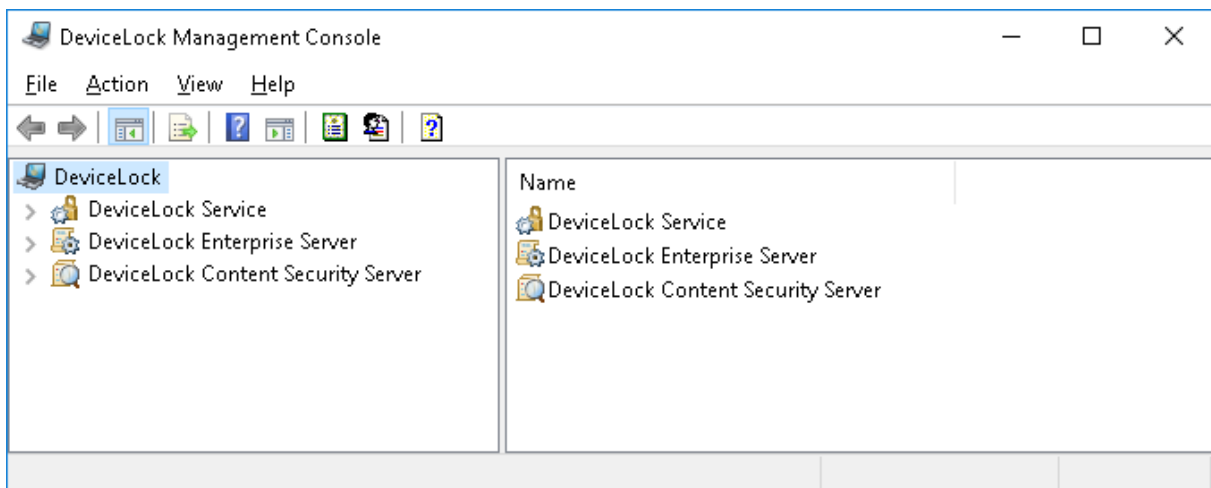


Alternatively, you can start MMC and add the DeviceLock Management Console snap-in:

1. Run **mmc** from a command prompt, or use the **Run** menu to execute this command.
2. Open the **File** menu, and then click **Add/Remove snap-in**.
3. Select **DeviceLock Management Console** from the list, and then click **Add**.
4. Click **OK**.

## Interface

DeviceLock Management Console has a user-friendly, easy-to-use standard interface provided by Microsoft Management Console (MMC). At any time, you can press the F1 key to get context-specific help.



DeviceLock Management Console consists of a window divided into two panes. The left pane contains the console tree; the right pane contains details. When you select an item in the console tree, information about that item is displayed in the details pane.

There are three independent parts in DeviceLock Management Console:

1. **DeviceLock Service** - Allows you to connect to and manage DeviceLock Services running on remote and local computers.
2. **DeviceLock Enterprise Server** - Allows you to connect to and manage DeviceLock Enterprise Servers running on remote and local computers.
3. **DeviceLock Content Security Server** - Allows you to connect to and manage DeviceLock Content Security Servers running on remote and local computers.

## DeviceLock root node

This root node represents DeviceLock in the management console.

The shortcut menu on the **DeviceLock** node in DeviceLock Management Console provides the following commands:

- **Certificate Generation Tool** - Starts a tool for generating DeviceLock Certificates. See [Generating DeviceLock Certificates](#) for details.

- **DeviceLock Signing Tool** - Starts a tool for granting users temporary access to requested devices and sign DeviceLock Service settings files. See [DeviceLock Signing Tool](#) for details.
- **About DeviceLock** - Displays a dialog box with information about the DeviceLock version and licenses.

In addition to these commands, the shortcut menu on the **DeviceLock Settings** node in [DeviceLock Service Settings Editor](#) or **DeviceLock** node in [DeviceLock Group Policy Manager](#) provides the following commands:

- **Undefine Entire Policy** - Resets all parameters to the unconfigured state. This command has the same effect as resetting all parameters one by one.
- **Undefine ContentLock Policy** - Resets all parameters specific to ContentLock (all Content-Aware Rules except those based on file types) to the unconfigured state.
- **Undefine NetworkLock Policy** - Resets all parameters specific to NetworkLock to the unconfigured state.
- **Remove ContentLock Policy** - Removes all parameters specific to ContentLock (all Content-Aware Rules except those based on file types). Available only in [DeviceLock Service Settings Editor](#).
- **Remove NetworkLock Policy** - Removes all parameters specific to NetworkLock. Available only in [DeviceLock Service Settings Editor](#).
- **Show Policy for Windows** - Causes the console to display only the settings related to DeviceLock Service for Windows.
- **Show Policy for Mac** - Causes the console to display only the settings related to DeviceLock Service for Mac.
- **Load Service Settings** - Loads settings from a DeviceLock Service settings file. You need to select a file created by saving DeviceLock Service settings in DeviceLock Service Settings Editor, DeviceLock Management Console, or DeviceLock Group Policy Manager. This could be a signed or non-signed file.
- **Save Service Settings** - Saves the DeviceLock Service current settings to a settings file. Later this file can be loaded to DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor. This file can also be sent to users whose computers are not on-line and thus out-of-reach via management consoles. To avoid tampering with the settings file, it should be signed using [DeviceLock Signing Tool](#). See also [Settings file save options](#).
- **Save & Sign Service Settings** - Saves the DeviceLock Service current settings to a settings file and signs it the private key of the last-used DeviceLock certificate. This command is unavailable if DeviceLock Signing Tool has never used a DeviceLock certificate's private key. See also [Settings file save options](#).
- **Create MSI Package** - Creates a custom MSI package for installing DeviceLock Service with the settings identical to the DeviceLock Service current settings.  
When using this command, you first need to select a source MSI package for DeviceLock Service. This may be one of MSI packages that ship with DeviceLock (such as DeviceLock Service.msi and DeviceLock Service x64.msi).

Then you need to specify the name of the resultant (target) MSI package that will be generated based on the source MSI package and the DeviceLock Service current settings.

Later this custom MSI package can be used to deploy DeviceLock Service across the network with predefined policies (see [Installation via Group Policy](#)).

---

#### Note

When a custom MSI package is used to deploy DeviceLock Service via Group Policy, these service settings held in that package are not applied to client computers if any one of the following conditions is true:

- The default security is disabled on remotely running DeviceLock Services.
  - The GPO applied to client computers has the **Override Local Policy** setting enabled.
- 

The **Create MSI Package** menu item is unavailable if Microsoft Windows Installer (version 1.0 or later) is not installed on the local computer.

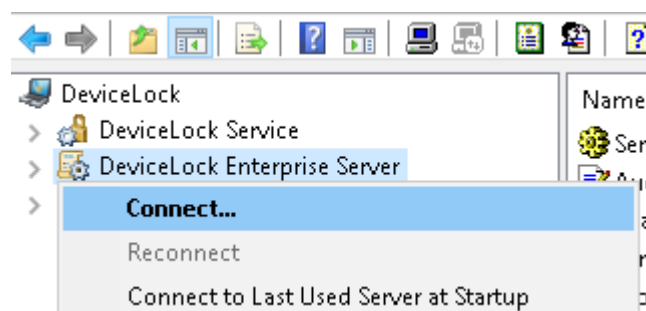
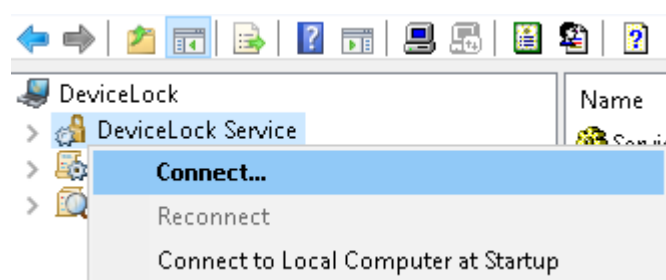
## DeviceLock Service node

The shortcut menu of the **DeviceLock Service** node depends upon the console you are using:

- In the DeviceLock Management Console, the menu provides commands for managing the DeviceLock Service to which the console is connected. See [Managing DeviceLock Service for Windows](#) for details.
- In the [DeviceLock Service Settings Editor](#), the menu provides the same commands as the menu on the [DeviceLock root node](#).

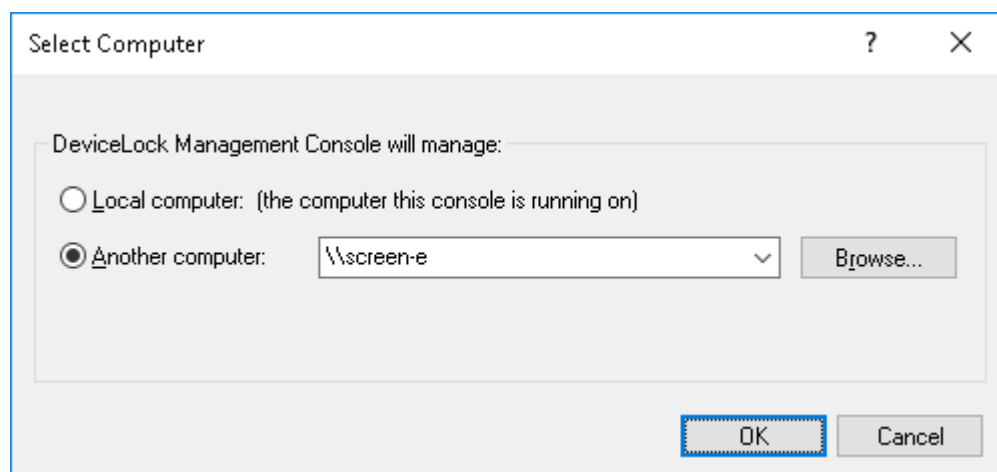
## Connecting to Computers

First of all, you should connect to the computer running DeviceLock Service, DeviceLock Enterprise Server, or DeviceLock Content Security Server. Use the **Connect** command on the shortcut menu or the respective button on the toolbar.



You can simultaneously connect to DeviceLock Service, DeviceLock Enterprise Server, and DeviceLock Content Security Server even if they are running on different computers.

In the dialog box that appears when selecting the **Connect** command, choose the **Local computer** option to connect to the computer on which the console is currently running. To connect to a different computer, choose the **Another computer** option, and specify the computer's name or IP address. Precede the computer name with 2 backslashes, such as \\computer\_name. Click the **Browse** button to select the desired computer from a list.



To connect to a computer where DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server is configured to use a fixed port, add the port number in square brackets after the computer name, such as \\computer\_name[port\_number].

Click **OK** to connect to the selected computer.

---

#### Note

Make sure that the remote computer is accessible from the computer running DeviceLock Management Console. The remote computer must run a DeviceLock-compatible operating system and it must have the TCP/IP protocol properly set up. If a firewall (including Windows Firewall) is enabled on the remote computer, it must be configured to allow connection to DeviceLock Service, DeviceLock Enterprise Server and/or DeviceLock Content Security Server. For further details, see the DeviceLock article at [kb.acronis.com/content/66460](https://kb.acronis.com/content/66460).

When installing, DeviceLock Service, as well as DeviceLock Enterprise Server and DeviceLock Content Security Server, automatically add themselves to the exception list of Windows Firewall.

---

When attempting to connect to a computer where DeviceLock Service is not installed or is outdated, DeviceLock Management Console prompts to install or update the service. For more information on remote service deployment, see the [Installation via DeviceLock Management Console](#) section of this manual.

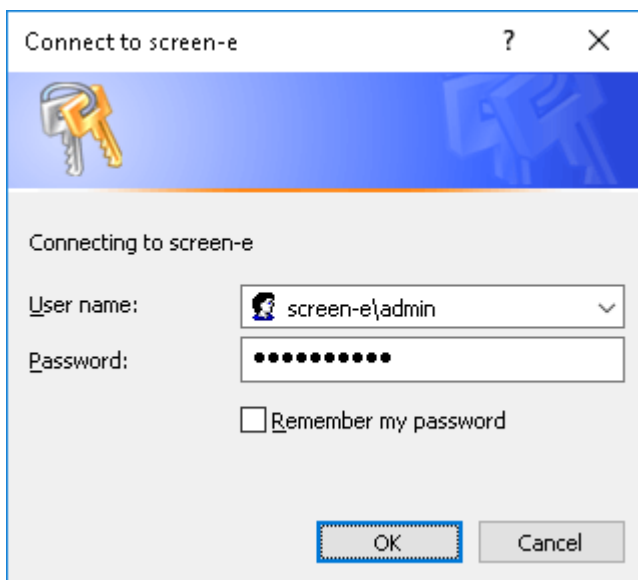
The following warning message appears when connecting to a computer where DeviceLock Service is in Group Policy mode: "This machine is configured to use Group Policy settings. You can switch it to the Local Policy mode. In this case Group Policy settings will be replaced by Local Policy settings."



When in Group Policy mode, DeviceLock Service receives its settings from the GPO, so changes to these settings made using DeviceLock Management Console will be lost upon a scheduled Group Policy update. For more information, see the [Use Group/Server Policy](#) parameter description in the [Service Options](#) section of this manual.

The following error message appears when attempting to connect to a computer where DeviceLock Enterprise Server or DeviceLock Content Security Server is not installed or is stopped: “There are no endpoints available from the endpoint mapper.” To connect to DeviceLock Enterprise Server or DeviceLock Content Security Server, these servers must be properly installed and started on the target computer. For more information and installation instructions, see the [Installing DeviceLock Enterprise Server](#) and [Installing DeviceLock Content Security Server](#) sections of this manual.

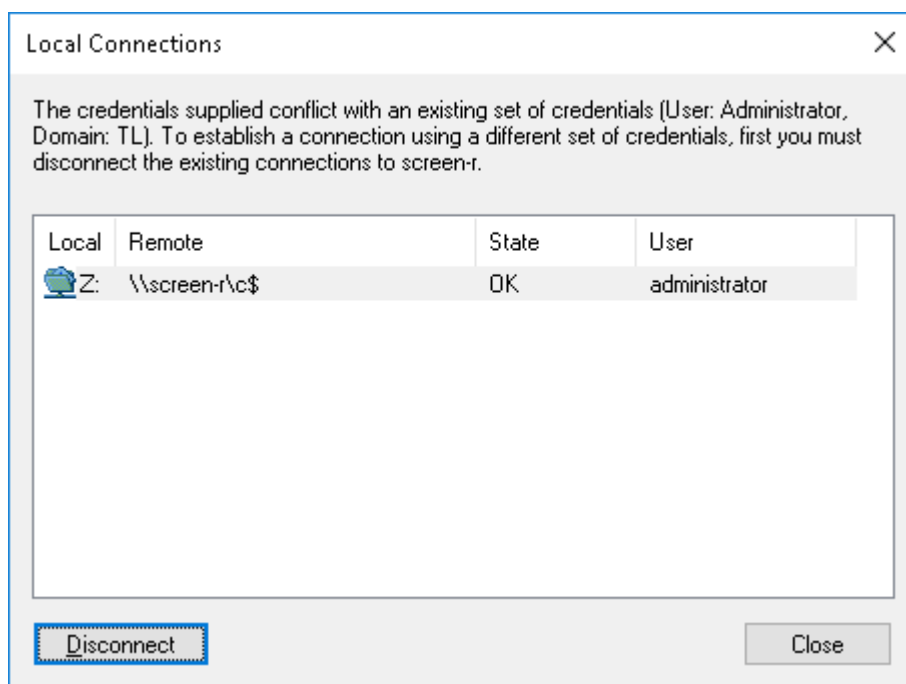
When connecting to a computer, DeviceLock Management Console checks to see if the current user has administrator rights on that computer. If the current user does not have sufficient rights, a dialog box appears to enter the name and password of another user.



In the dialog box that appears, specify the name and password of the user with administrator rights. This user should also be a DeviceLock administrator if the explicit list of administrators is configured for DeviceLock Service, DeviceLock Enterprise Server, or DeviceLock Content Security Server.

A “credentials conflict” may occur when you access a resource on a computer (such as a mapped network drive, shared folder, etc.) as a certain user, and then provide the name and password of another user to connect DeviceLock Management Console to that computer. Windows does not allow multiple connections to the same computer using different accounts, and returns the following error message: “The credentials supplied conflict with an existing set of credentials.” To resolve the conflict, you must disconnect existing connections to the remote computer.

When DeviceLock Management Console detects a credentials conflict, it lists connections that exist on your local computer, allowing you to disconnect them.



In the dialog box that appears, select all existing connections to the computer you want to connect to, and click the **Disconnect** button. Click **Close**, and then try to connect to that computer again.

---

#### Note

Sometimes disconnecting an existing connection fails, which prevents a connection using an alternative account. In this case, use the **Run as different user** command to start the console under an account with administrator rights on DeviceLock Service, DeviceLock Enterprise Server, and/or DeviceLock Content Security Server. This command appears on the shortcut menu if you right-click while holding down the Shift key.

---

## Possible connection errors

When you're trying to connect to a computer with DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server you may receive some of these errors:

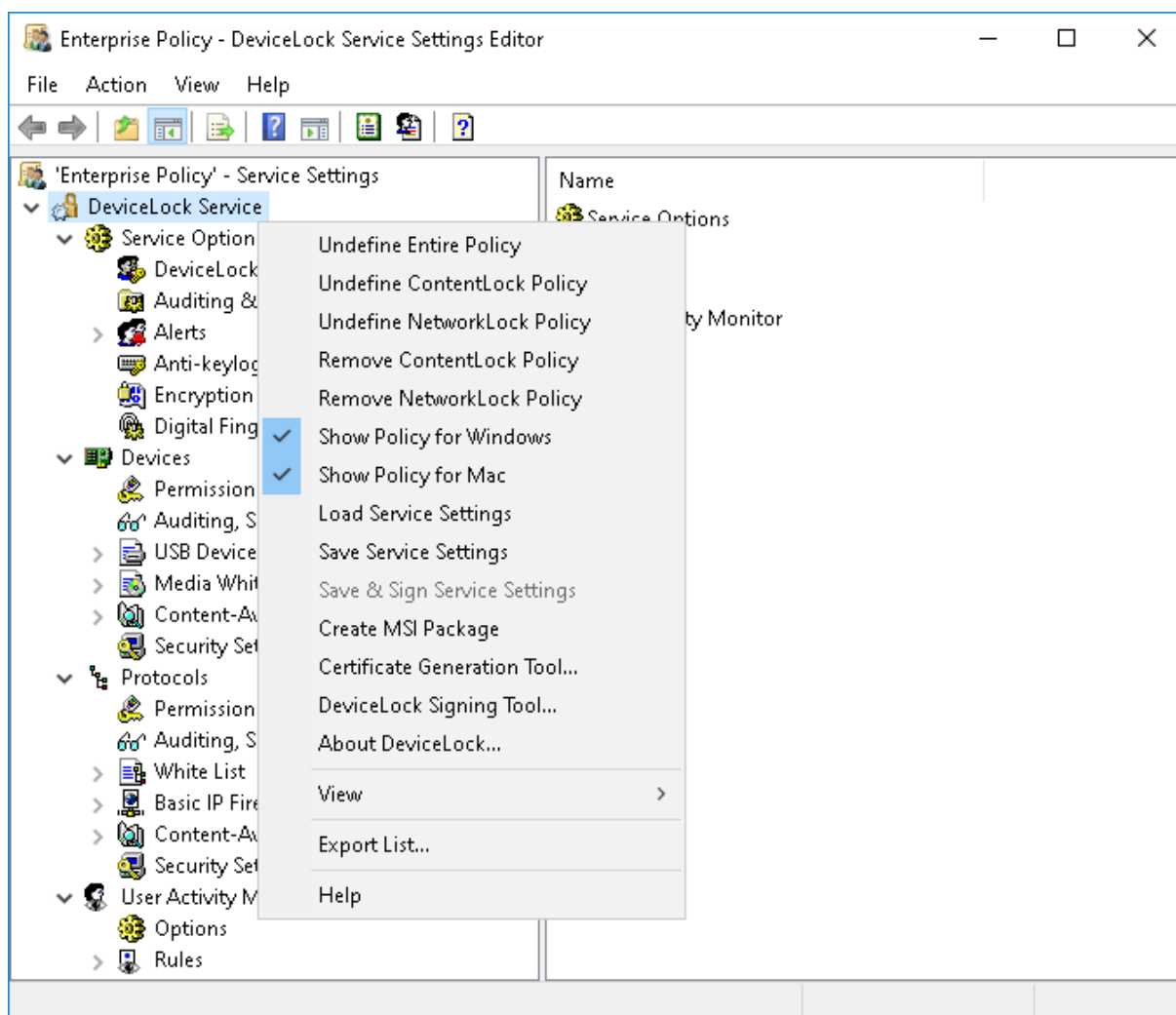
- **(1722) The RPC server is unavailable** - You're trying to connect to a computer that either does not exist (the wrong name or IP address) or is not accessible. Make sure that the computer name you've specified is correct. Try to ping this computer by its name and IP address and connect to it using any standard Windows administrative tool (such as Computer Management, Services and so on). Make sure that this computer is working under a DeviceLock-compatible OS. Also, it is possible that a firewall is blocking access to this computer. You would need to configure your firewall to allow some ports needed for DeviceLock. You could also instruct DeviceLock to use the fixed TCP port, making it easier to configure a firewall. By default, DeviceLock Service, DeviceLock Enterprise Server and DeviceLock Content Security Server are using 9132, 9133 and 9134 ports thereafter. Also, please note that DeviceLock Service automatically adds itself to the exception list of Windows Firewall.

- **(1753) There are no more endpoints available from the endpoint mapper** - You're trying to connect to a computer where DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server is not accessible. First of all, make sure that DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server is installed and started on the remote computer.  
It is possible that this computer was just started and Windows is still initializing its services. The Remote Procedure Call (RPC) service may not be running yet.  
It is also possible that the firewall is blocking access to DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server (see error description 1722 above). For instructions on configuring the firewall to support Remote Procedure Call, see Microsoft's article at [docs.microsoft.com/windows/security/threat-protection/windows-firewall/create-inbound-rules-to-support-rpc](https://docs.microsoft.com/windows/security/threat-protection/windows-firewall/create-inbound-rules-to-support-rpc).  
More on troubleshooting Remote Procedure Call errors see in Microsoft's article at [docs.microsoft.com/windows/client-management/troubleshoot-tcpip-rpc-errors](https://docs.microsoft.com/windows/client-management/troubleshoot-tcpip-rpc-errors).
- **(5) Access is denied** - You don't have enough privileges on the remote computer. Make sure that DeviceLock Management Console is trying to connect to the remote computer under a user with local administrator privileges on that computer.  
You may also need to run DeviceLock Management Console under a different user that can authenticate on the remote computer as a local admin.
- **(7045) You must have administrative privileges to perform this operation** - You don't have sufficient privileges to access DeviceLock Service, DeviceLock Enterprise Server or DeviceLock Content Security Server because the user is not in the list of DeviceLock Administrators. Make sure that DeviceLock Management Console is trying to connect to the remote computer under the user that is in the list of DeviceLock Administrators on that computer.

## DeviceLock Service Settings Editor

DeviceLock Service Settings Editor is used for creating and modifying files with settings, permissions, audit, shadowing rules and alerts for DeviceLock Service (DeviceLock Service settings files).

DeviceLock Service Settings Editor installs together with the other management consoles.



There is almost no difference between the procedures for defining policies via DeviceLock Management Console versus via DeviceLock Service Settings Editor. For more information, see [Managing DeviceLock Service for Windows](#).

Comparing to DeviceLock Management Console, in the DeviceLock Service Settings Editor you can:

- Manage DeviceLock Service settings without connecting to any computer with DeviceLock Service. DeviceLock Service Settings Editor modifies and stores settings in external files and allows you to create/edit policies offline. It works similar to DeviceLock Group Policy Manager but instead of GPOs it uses settings files.
- Reset any parameter (or all parameters at once) to the undefined state. All undefined parameters are ignored when the policy is applied to DeviceLock Service.
- Remove the ContentLock policy and/or NetworkLock policy from a settings file, which causes the ContentLock and/or NetworkLock settings to be undefined when you apply that file to DeviceLock Service. For an overview of ContentLock and NetworkLock, see [ContentLock and NetworkLock](#) earlier in this document.
- Remove any offline policy settings (permissions, audit, shadowing rules and alerts, white lists, etc.) for both devices and protocols in order to enforce regular ones in this policy file.

## Creating or Modifying a Policy

To create a new policy from scratch, just run DeviceLock Service Settings Editor and start making changes in its default (empty) policy.

If you want to modify an existing policy, you should load the DeviceLock Service settings file with that policy to DeviceLock Service Settings Editor using the **Load Service Settings** shortcut menu command and then make desired changes.

---

### Note

The name of the settings file loaded to the editor is displayed in the caption of the console window (such as Service Settings - [date time] - DeviceLock Service Settings Editor).

---

If you create a new policy from scratch, you should use the **Save Service Settings** command from the shortcut menu to save it to a file. Alternatively, you can use the **Save & Sign Service Settings** command to save the policy to a file and automatically sign it with the most recent DeviceLock Certificate (the private key). The **Save & Sign Service Settings** command is unavailable when the [DeviceLock Signing Tool](#) has no previously loaded private key. It is also possible not to store SID (security identifiers) in the settings file (see [Settings file save options](#)).

Later files with policies created using DeviceLock Service Settings Editor can be loaded via DeviceLock Management Console and/or DeviceLock Group Policy Manager.

Also, files with policies can be sent to users whose computers are not online and thus out-of-reach via management consoles. To avoid unauthorized modification these files should be signed with the DeviceLock Certificate (the private key) using the DeviceLock Signing Tool. For more information, see [Service Settings](#) in the [DeviceLock Signing Tool](#) section of this manual.

If you modify an existing policy file, DeviceLock Service Settings Editor automatically saves your changes.

---

### Note

Only settings that are explicitly defined in a policy file apply to client computers. All policy settings that have the **Not Configured** state are ignored by client computers.

---

DeviceLock Service Settings Editor is also used in the Set Service Settings plug-in of DeviceLock Enterprise Manager. This plug-in runs DeviceLock Service Settings Editor as an external application and opens it with the service settings file selected in the plug-in's settings dialog box.

When you make any policy changes (change parameters, set permissions, define white lists, etc.) in the service settings file passed to the editor by the plug-in, DeviceLock Service Settings Editor automatically saves them to this file. As soon as you finish modifying the policy just close DeviceLock Service Settings Editor and return to the plug-in's settings dialog box.

For more information, see [Set Service Settings](#) plug-in description in the [DeviceLock Enterprise Manager](#) section of this manual.

## Settings file save options

When you save a settings file, you can choose from the following options:

- **DeviceLock Settings Files** - The saved file will contain most complete info about users that are assigned DeviceLock policies and rules in this file, including user, group, domain and computer names as well as SID (security identifiers).
- **DeviceLock Settings Files - Textual Fully Qualified User Name** - The saved file will not contain security identifiers, except identifiers of well-known local users and groups (such as SYSTEM, Administrators, etc). Account names will be specified in the format <domain name>\<user name>.
- **DeviceLock Settings Files - Textual User Name** - The saved file will not contain security identifiers, except identifiers of well-known local users and groups. Account names will be specified in the format <user name>, without indicating the domain or computer name.

Saving a settings file without security identifiers and domain/computer names may be required in a situation where you need to apply the file to different stand-alone computers each of which has the same set of local user names. In this case, the file should identify users by name, without specifying security identifiers or domain/computer names; otherwise, DeviceLock Service would be unable to resolve user names on a computer other than the one on which the given settings file was saved.

## DeviceLock Group Policy Manager

In addition to standard ways of managing permissions and settings via [DeviceLock Consoles and Tools](#), there is a more powerful tool - permissions, audit rules and other DeviceLock Service settings can be configured and deployed via Group Policy in Active Directory environments, which allows administrators to centrally control configuration of DeviceLock Service on domain-joined computers.

Group Policy support makes it possible to administer DeviceLock Service by configuring and applying policy settings in the Group Policy Management Console (GPMC).

Tight integration into Active Directory is a very important function of DeviceLock as it makes the management and deployment of the DeviceLock Service easier in large networks, without the need to install additional servers. DeviceLock does not require its own server components to manage computers on the network, instead it uses the standard features of the Active Directory service.

Group Policy can be used to:

- Install DeviceLock Service on all the computers on a network, even those that are not currently running and new computers that are just connecting to the network. For more information, see [Installation via Group Policy](#).
- Control and configure DeviceLock Service on a large number of computers in different domains/organizational units simultaneously. Even if some computers are turned off or absent

on the network, the DeviceLock Service settings will be automatically deployed on such computers after they are started and connected to the network.

- View the policy currently being applied and predict what policy would be applied. For more information, see [Using Resultant Set of Policy \(RSOP\)](#).

---

**Note**

To manage DeviceLock via Group Policy, Active Directory must be installed and configured. For Active Directory installation and configuration instructions, refer to Microsoft's documentation.

---

## How Group Policy is applied

Policy is applied when the computer starts up. When a user turns on the computer, the system applies DeviceLock's policy.

Policy can be optionally reapplied on a periodic basis. By default, policy is reapplied every 90 minutes. To set the interval at which policy will be reapplied, use the Group Policy Object Editor. For more information, refer to the Microsoft Knowledge Base at [support.microsoft.com/kb/203607](https://support.microsoft.com/kb/203607).

Policy can also be reapplied on demand. To refresh the current policy settings immediately, administrators can call the `gpupdate.exe /force` command-line utility provided by Windows.

When applying policy, the system queries the directory service for a list of Group Policy Objects (GPOs) to process. Each GPO is linked to an Active Directory container to which the computer or user belongs. By default, the system processes the GPOs in the following order: local, site, domain, then organizational unit. Therefore, the computer receives the policy settings of the last Active Directory container processed.

When processing the GPO, the system checks the access-control list (ACL) associated with the GPO. If an access-control entry (ACE) denies the computer access to the GPO, the system does not apply the policy settings specified by the GPO. If the ACE allows access to the GPO, the system applies the policy settings specified by the GPO.

## Standard GPO inheritance rules

Any unconfigured settings anywhere in a GPO can be ignored since they are not inherited down the tree; only configured settings are inherited. There are three possible scenarios:

- A parent has a value for a setting, and a child does not.
- A parent has a value for a setting, and a child has a non-conflicting value for the same setting.
- A parent has a value for a setting, and a child has a conflicting value for the same setting.

If a GPO has settings that are configured for a parent Organizational Unit, and the same policy settings are unconfigured for a child Organizational Unit, the child inherits the parent's GPO settings. That makes sense.

If a GPO has settings configured for a parent Organizational Unit that do not conflict with a GPO on a child Organizational Unit, the child Organizational Unit inherits the parent GPO settings and applies its own GPOs as well.

If a GPO has settings that are configured for a parent Organizational Unit that conflict with the same settings in another GPO configured for a child Organizational Unit, then the child Organizational Unit does not inherit that specific GPO setting from the parent Organizational Unit. The setting in the GPO child policy takes priority, although there is one case in which this is not true.

If the parent disables a setting and the child makes a change to that setting, the child's change is ignored. In other words, the disabling of a setting is always inherited down the hierarchy.

## Recommendations

When the [Windows BitLocker To Go](#) option is enabled (see [Encryption](#)), the DeviceLock Service can prevent the application of administrative templates from GPOs, because this option prevents enabling the Group Policy setting "Deny writing to removable drives not protected by BitLocker" in Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives. As a result, any Group Policy with a conflicting value for this setting will not be applied to the computer.

To resolve this issue, disable the option [Windows BitLocker To Go](#) (enabled by default). If DeviceLock Service settings come from a GPO or from a server policy object (see [DeviceLock Enterprise Server Policies](#)), then the [Windows BitLocker To Go](#) option must be explicitly disabled in that object; otherwise, this option will be set by default, that is, it will be enabled. If using local settings for the DeviceLock Service, just disable this option in the DeviceLock Management Console.

## Getting started with DeviceLock Group Policy Manager

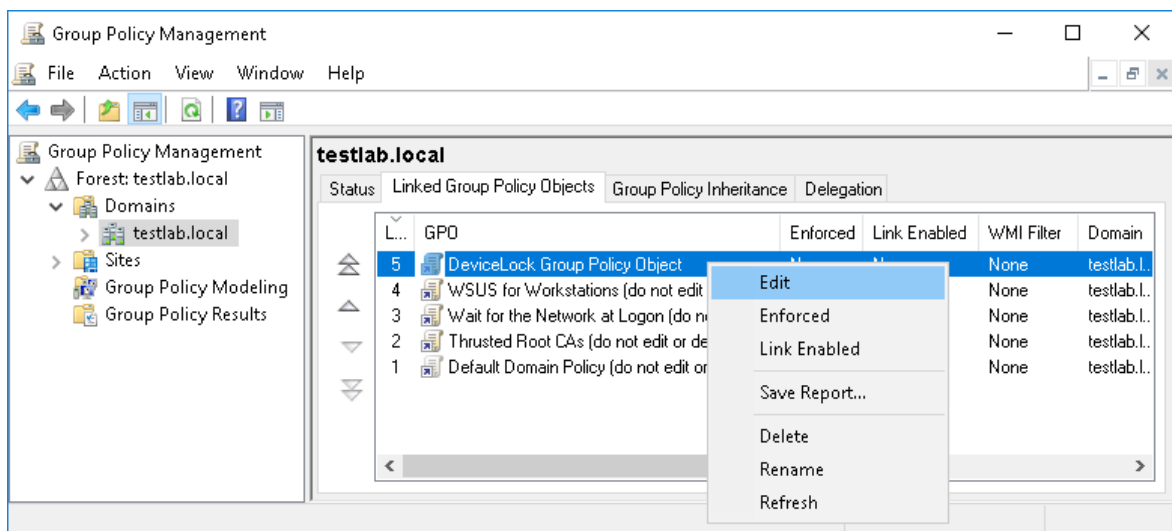
DeviceLock Group Policy Manager integrates into the Windows Group Policy Object (GPO) editor. To use DeviceLock Group Policy Manager on your local PC rather than on the domain controller, you install the Group Policy Management console (GPMC).

For Windows Server 2003 or Windows XP you can download the Group Policy Management console at [microsoft.com/download/details.aspx?id=21895](https://microsoft.com/download/details.aspx?id=21895). On a later version of the Windows client operating system, you should install Remote Server Administration Tools (for instructions see Microsoft's article at [support.microsoft.com/kb/2693643](https://support.microsoft.com/kb/2693643)).

Use the following steps to access DeviceLock Group Policy Manager:

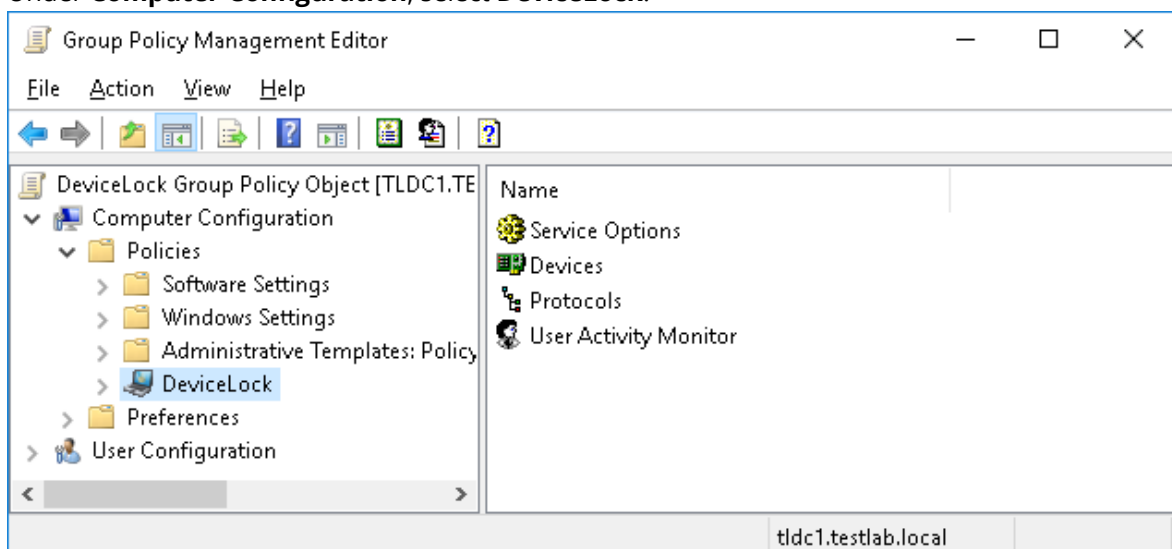
1. Start the Group Policy Management console.
2. In the console tree, select your Active Directory domain.
3. On the **Linked Group Policy Objects** tab in the details pane, right-click the desired Group Policy object, and then click **Edit**.





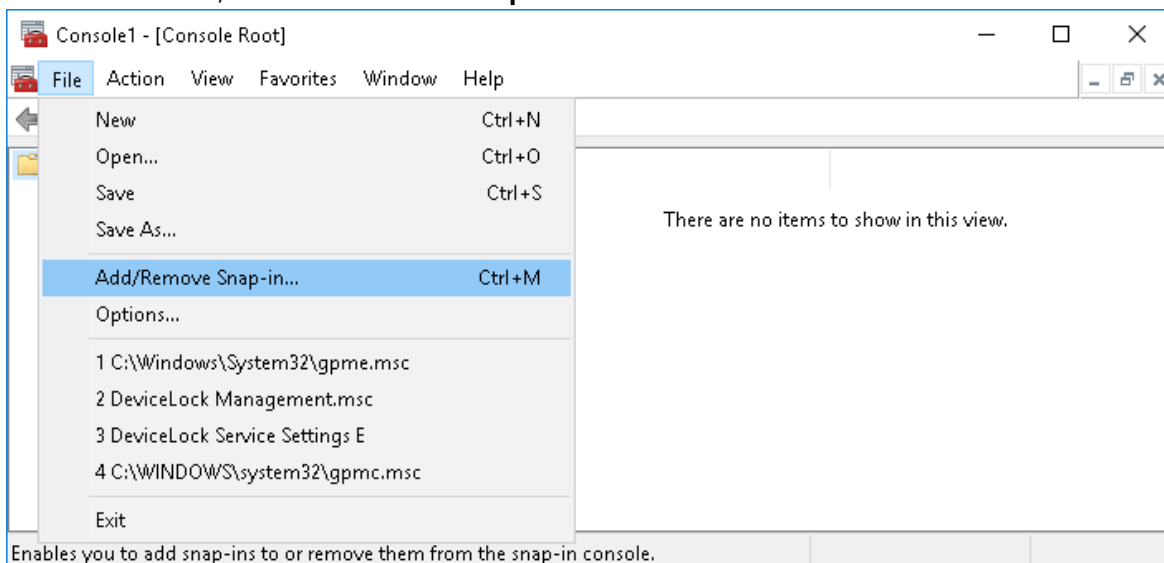
If you wish to create a new Group Policy object, right-click the domain in the console tree and choose the following command: **Create a GPO in this domain, and Link it here.**

4. Wait while the Group Policy Management editor starts. It may take up to several seconds.
5. Under **Computer Configuration**, select **DeviceLock**.

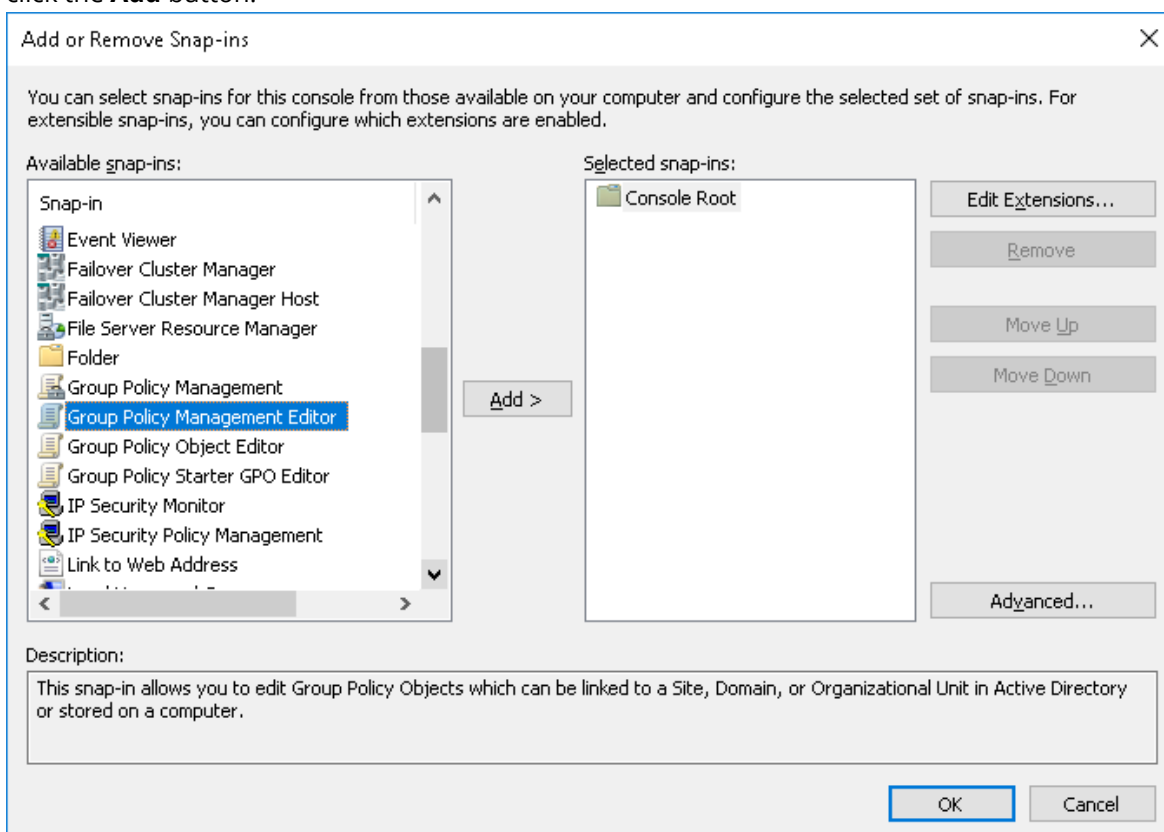


Alternatively, you can start MMC and open the Group Policy Management Editor snap-in as follows:

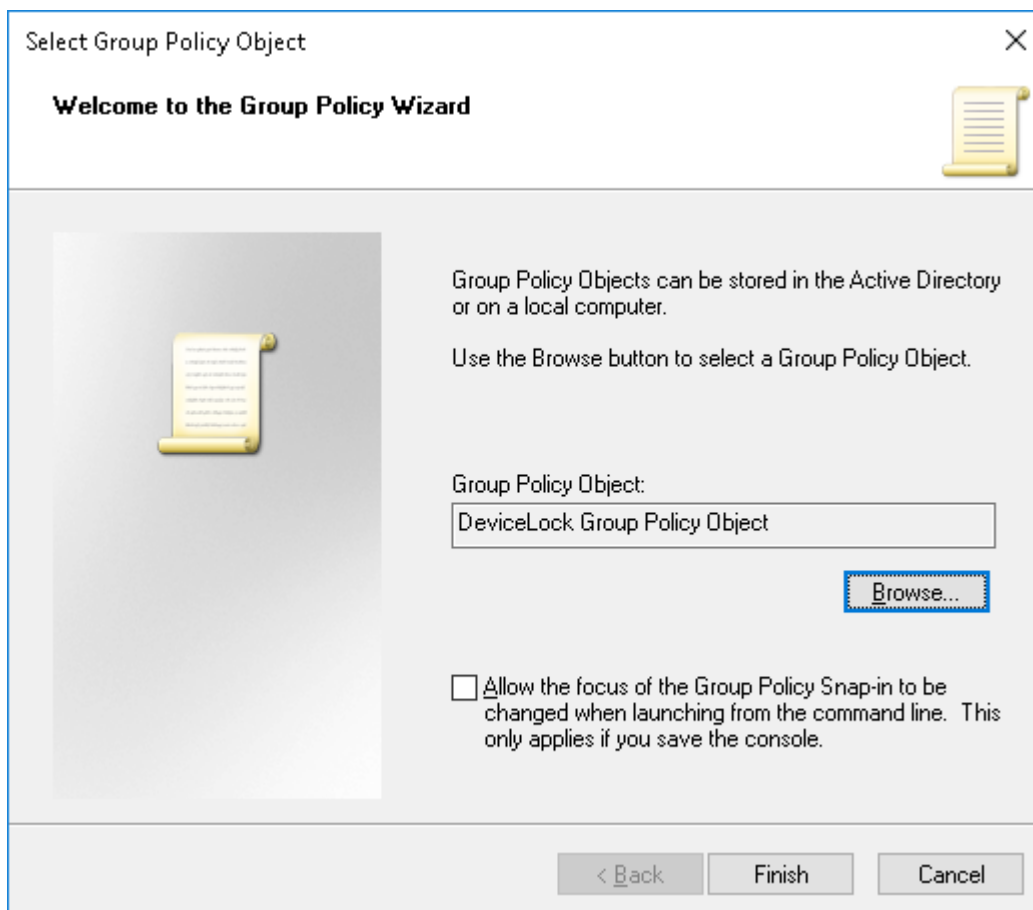
1. Run **mmc** from the command line or use the **Run** menu to execute this command.
2. On the **File** menu, click **Add/Remove snap-in**.



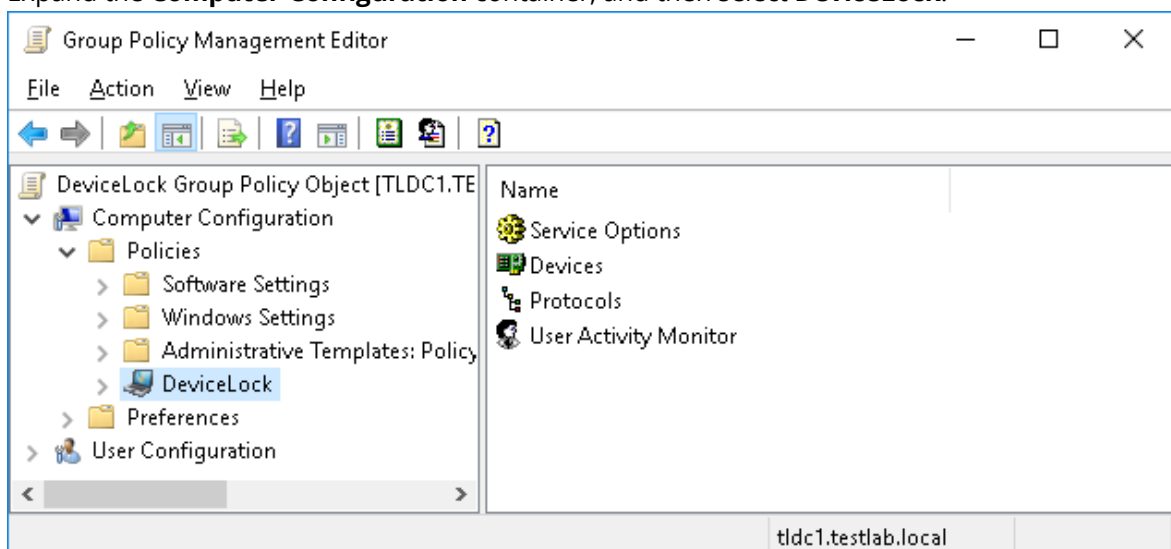
3. In the dialog box that appears, select the **Group Policy Management Editor** snap-in, and then click the **Add** button.



4. Click the **Browse** button to select the desired Group Policy object from your Active Directory domain, and then click **Finish**.



5. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
6. Expand the **Computer Configuration** container, and then select **DeviceLock**.



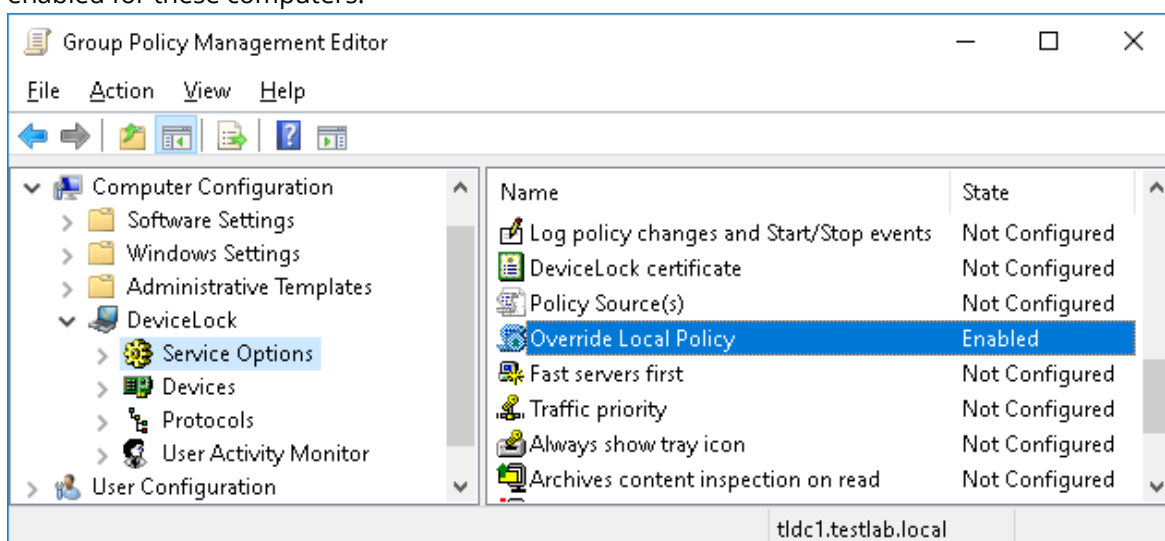
## Using DeviceLock Group Policy Manager

There is almost no difference between the procedure of managing DeviceLock Service via DeviceLock Management Console and via DeviceLock Group Policy Manager. For more information, see [Managing DeviceLock Service for Windows](#).

It is impossible to manage DeviceLock Enterprise Server and view audit and shadow logs using DeviceLock Group Policy Manager. For such operations you should use [DeviceLock Consoles and Tools](#).

DeviceLock Service management via DeviceLock Group Policy Manager includes four additional features in comparison to DeviceLock Management Console:

1. **Override Local Policy** - If you want to prevent changes to settings, permissions and audit rules for individual computers that bypass Group Policy or [DeviceLock Enterprise Server Policies](#), enable **Override Local Policy** in **Service Options**. This enforces the Group Policy or Server Policy mode for all the computers in the Policy Object, so that the Local Policy mode cannot be enabled for these computers.



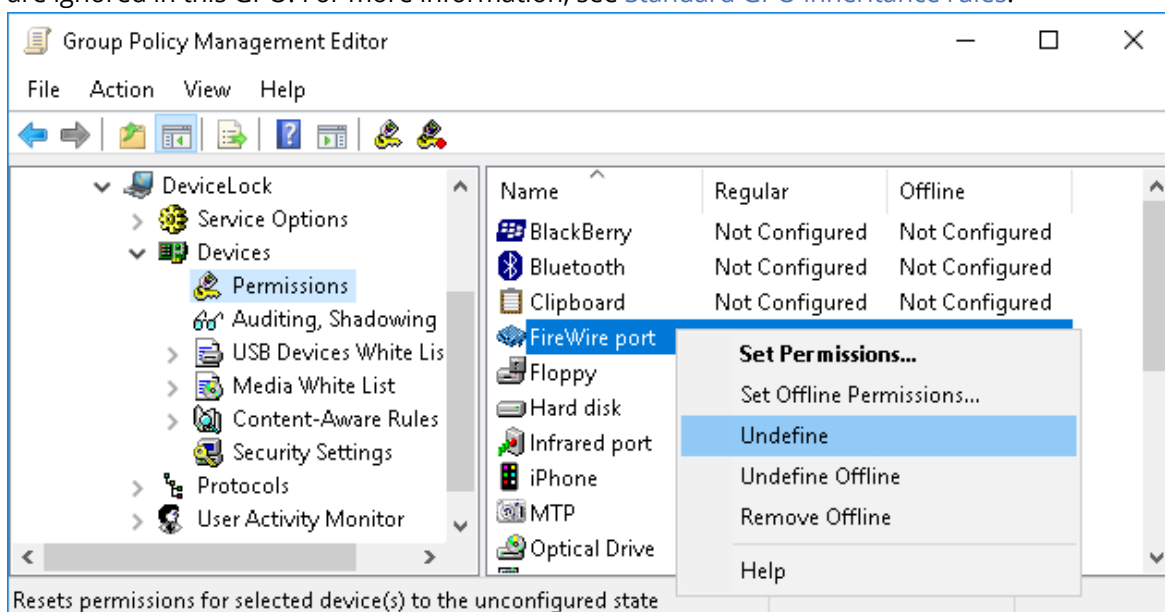
If **Override Local Policy** is enabled, the **Use Group/Server Policy** parameter in Service Options in the DeviceLock Management Console or DeviceLock Enterprise Manager cannot be disabled. The following table shows how different settings of the **Use Group/Server Policy** parameter and the **Override Local Policy** parameter affect the policy application mode:

Use Group/Server Policy	Override Local Policy	Policy application mode
Disabled	Disabled	Only Local Policy is applied.
Enabled	Enabled	Only Group Policy or Server Policy is applied.
Enabled	Disabled	Group Policy or Server Policy is applied. Local Policy may be in effect until a subsequent replication of the Group Policy or Server Policy settings.

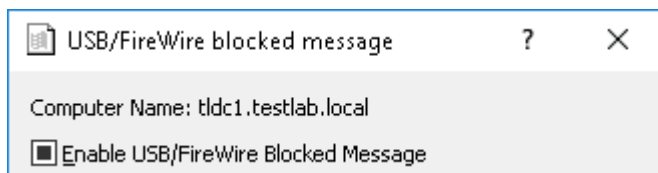
When setting the **Override Local Policy** parameter, consider the following:

- When **Override Local Policy** is disabled while **Use Group/Server Policy** is enabled, DeviceLock Service settings can be changed via DeviceLock Management Console or DeviceLock Enterprise Manager. However, Group Policy or Server Policy settings will eventually override these changes.

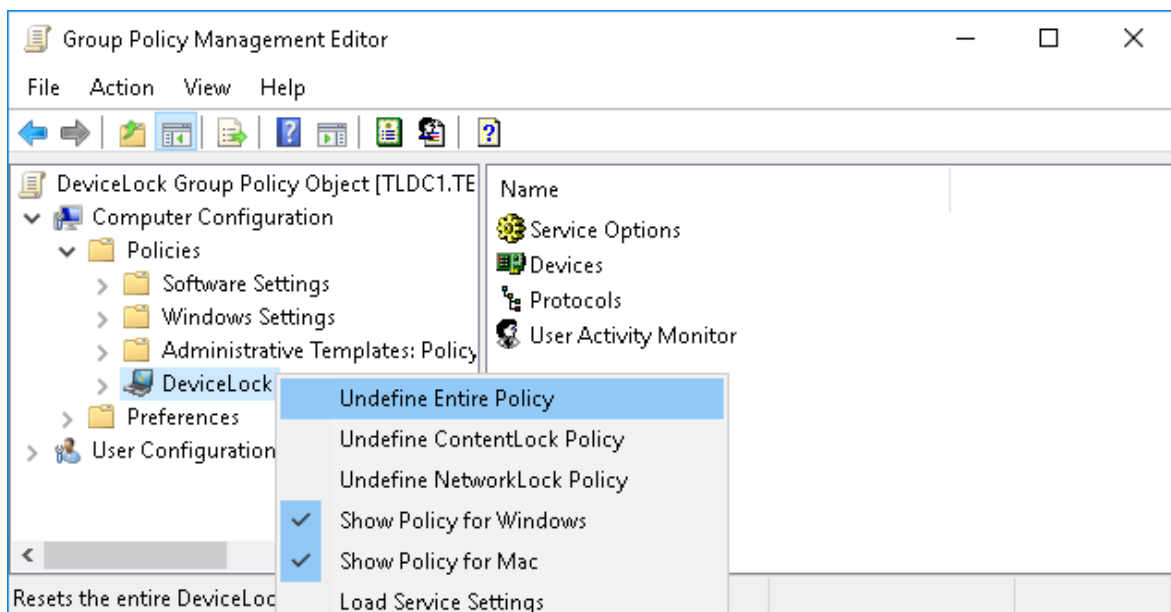
- When **Override Local Policy** is disabled, all changes to DeviceLock Service settings made via DeviceLock Management Console or DeviceLock Enterprise Manager take effect immediately.
2. **Undefine** - You can reset any parameter to the unconfigured state. All undefined parameters are ignored in this GPO. For more information, see [Standard GPO inheritance rules](#).



Use **Undefine** from the shortcut menu of any parameter to reset this parameter to the unconfigured state. Also, for some parameters, you can use the intermediate state of the check box to make it unconfigured.



3. **Undefine Entire Policy** - You can reset all parameters to the unconfigured state in one click. Selecting this has the same effect as resetting each parameter one by one (see above).



Use **Undefine entire policy** from the shortcut menu of **DeviceLock** to reset all parameters to the unconfigured state. A message that asks you to confirm the operation will appear: “Undefining the entire DeviceLock policy is an irreversible action. All DeviceLock settings will be lost. Are you sure you want to continue?”

4. **Remove Offline** - You can remove any offline policy settings (permissions, audit, shadowing rules and alerts, white lists, etc.) for both devices and protocols in order to enforce regular ones in this GPO. To do so, right-click any policy setting, and then click **Remove Offline**.

---

#### Note

In order to manage DeviceLock Service settings via Group Policy, DeviceLock Service must be installed and started on all the computers belonging to the GPO. For more information about the service installation, see [Deploying DeviceLock Service for Windows](#).

Also, do not forget that Group Policy is reapplied on a periodic basis (by default, every 90 minutes) so your changes do not take effect immediately. For more information, see [How Group Policy is applied](#).

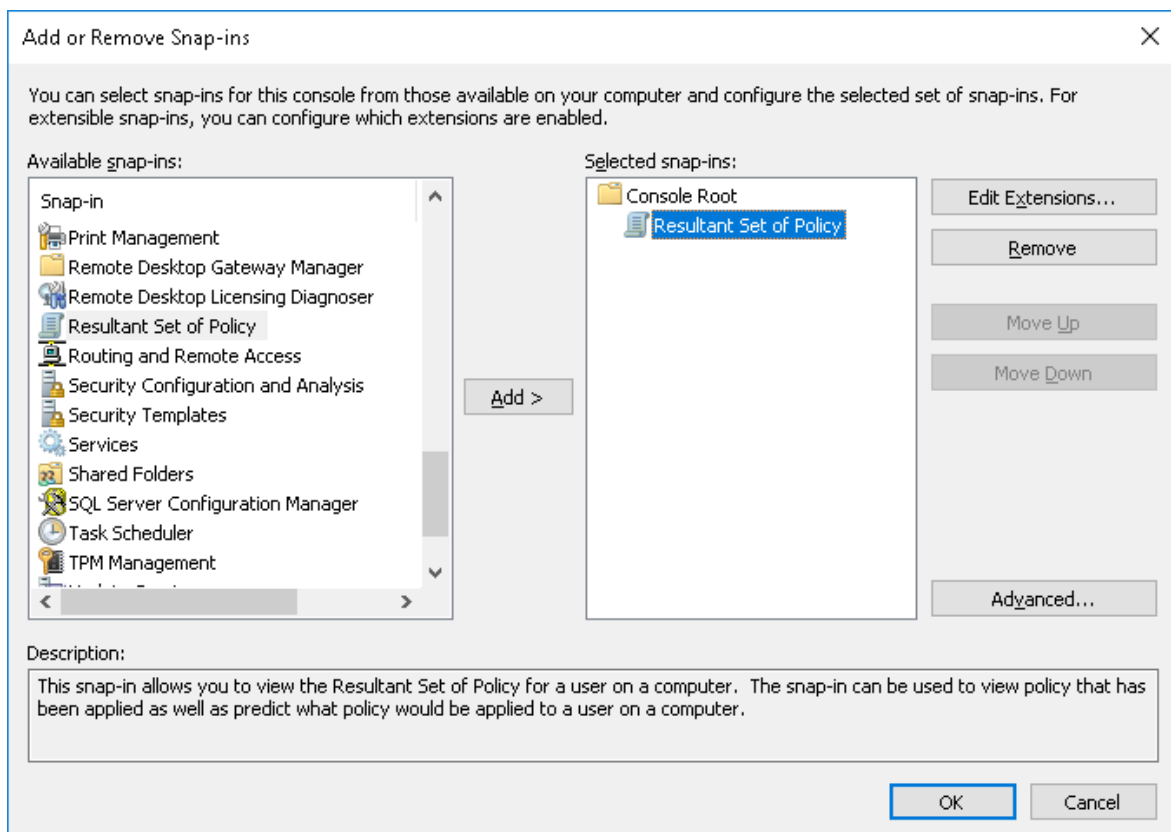
---

## Using Resultant Set of Policy (RSOP)

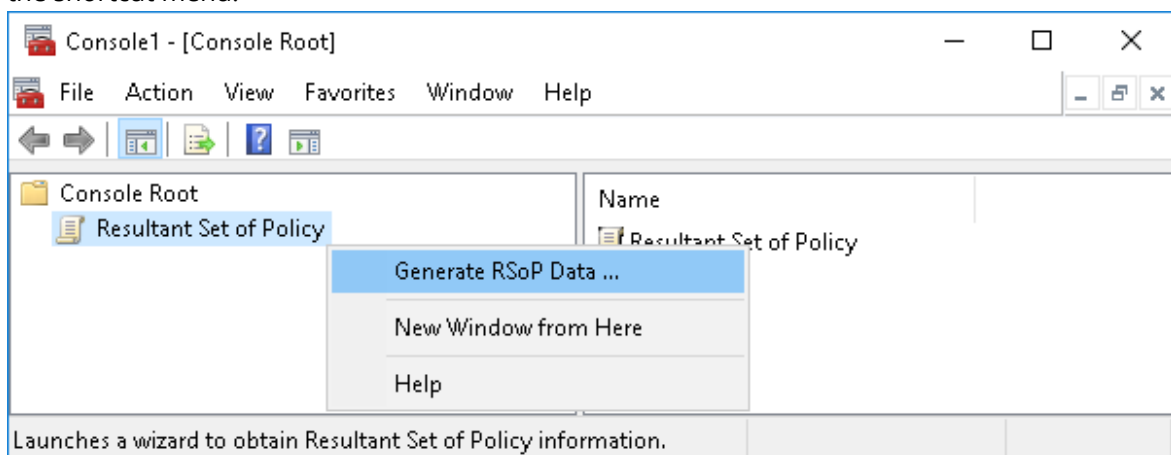
DeviceLock supports Resultant Set of Policy so you can use the standard Windows snap-in to view the DeviceLock policy currently being applied, as well as to predict what policy would be applied to a chosen computer.

To use RSOP, you should start MMC and add the Resultant Set of Policy snap-in manually:

1. Run **mmc** from the command line or use the **Run** menu to execute this command.
2. On the **File** menu, click **Add/Remove snap-in**.
3. In the dialog box that appears, select the **Resultant Set of Policy** snap-in, and then click the **Add** button.



4. Click **OK** to close the **Add or Remove Snap-ins** dialog box.
5. In the console tree, right-click **Resultant Set of Policy**, and then click **Generate RSoP Data** on the shortcut menu.



6. Go through the wizard that appears to collect the necessary data and build the resultant set of policy.
7. Expand the **Resultant Set of Policy** node in the console tree, and select **DeviceLock** under **Computer Configuration**.

Note that using RSoP you cannot modify the policy - all parameters are in the read-only mode.

RSoP is very useful when you need to understand which particular GPO will be applied to the computer.

For more information on Resultant Set of Policy, see Microsoft's article at [technet.microsoft.com/library/cc758010.aspx](https://technet.microsoft.com/library/cc758010.aspx).

## Using Group Policy to Manage DeviceLock Service for Mac

DeviceLock Service for Mac can retrieve configuration settings from Active Directory via DeviceLock Enterprise Server. In order to enable DeviceLock Service for Mac to receive settings from group policies, perform the following steps:

1. Register the Mac computer in the Windows domain.
2. Place the newly added computer into the required OU and configure policies according to your requirements.
3. Install DeviceLock Enterprise Server. No specific settings are required. Make sure that the computer hosting DeviceLock Enterprise Server has access to the domain controller with which the Mac computer is registered.
4. On the Mac computer, enter the address of DeviceLock Enterprise Server configured during the previous step.

Group policies will be applied to the Mac computer in the following cases:

- Upon system restart.
- Every hour.
- When the [DeviceLock Enterprise Server\(s\)](#) parameter is changed in [Service Options](#).
- Forced update is performed.

To perform the forced update, use the following command:

```
/Library/DeviceLockAgent/Utilities/DLAgentControl gpupdate
```

## DeviceLock Enterprise Manager

With DeviceLock Enterprise Manager, you can view and change security policies defined for device types and protocols; install, update and uninstall DeviceLock Service; and view audit and shadow logs for all the computers in a large network. We recommend using DeviceLock Enterprise Manager if you have a large network without Active Directory.

Based on a multi-threaded engine, using this console speeds up all activity for all the computers in the large network.

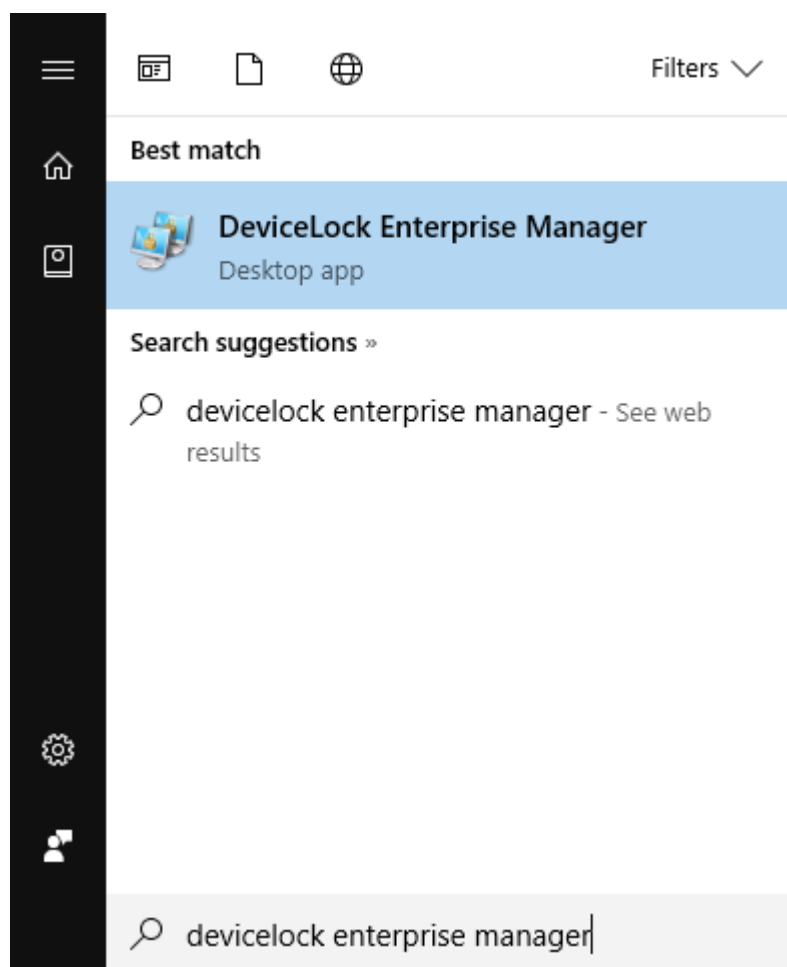
DeviceLock Enterprise Manager stores, compares and filters the data it receives from all the computers. Administrators can make "snapshots" of the systems for future comparison and notation of changes.

DeviceLock Enterprise Manager has a flexible plug-in based architecture that allows you to plug in necessary modules on demand. Each module (plug-in) performs a task and displays retrieved information in its own window.



For information on how to install DeviceLock Enterprise Manager, see [Installing Management Consoles](#) earlier in this manual.

To open DeviceLock Enterprise Manager, find and select that app on the Windows start page:

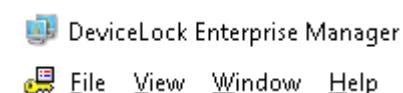


## Interface

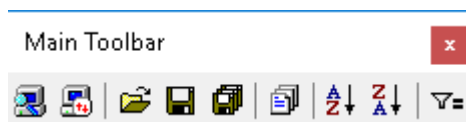
DeviceLock Enterprise Manager has a Multi Document Interface (MDI) structure, allowing you to keep each task in its own window.

The main window of DeviceLock Enterprise Manager can be resized. DeviceLock Enterprise Manager saves its size and position, and restores these at its next startup.

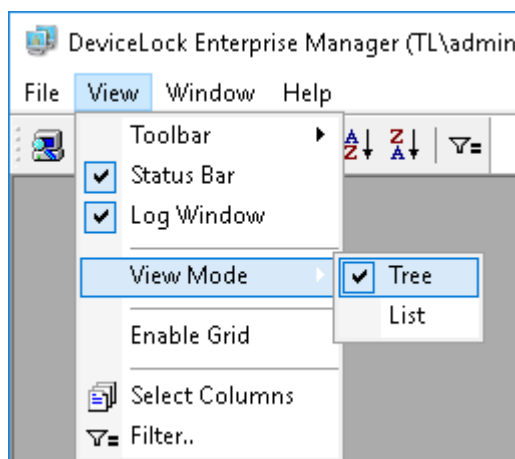
There is a menu at the top of the main window. Many functions are accessible through this menu:



To change the columns displayed in the plug-in's windows, click **Select Columns** on the **View** menu or click the appropriate button on the main toolbar.



By default, DeviceLock Enterprise Manager displays information received from the plug-ins in the form of a tree. However, information can also be displayed as a plain list. To change the mode, point to **View Mode** on the **View** menu and click either **Tree** or **List**. Please note that View Mode must be set for each plug-in individually.

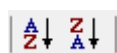


You can hide the status bar and/or the log window by deselecting appropriate items on the **View** menu. To enable the gridlines around items in the plug-in's window, click **Enable Grid** on the **View** menu. This mode sets for each plug-in individually.

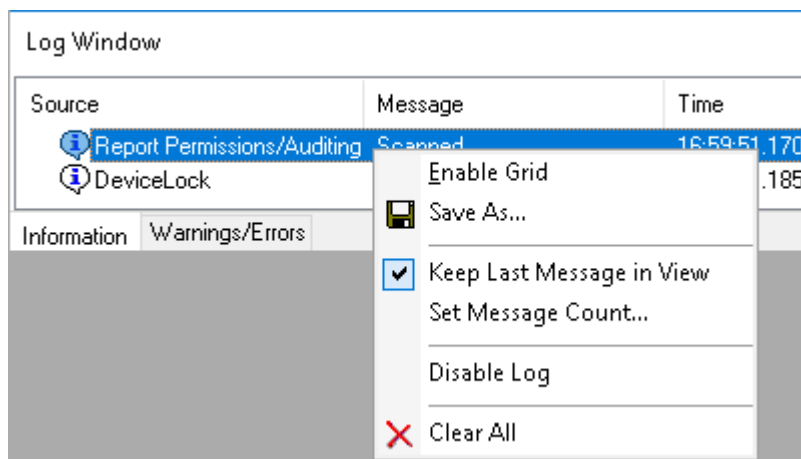
To sort data in any plug-in's window, click the column heading you want to sort by. To reverse the sort order, click the column heading a second time:



If you need to sort the top-level tree's items (such as domains and computers), use appropriate buttons on the main toolbar:



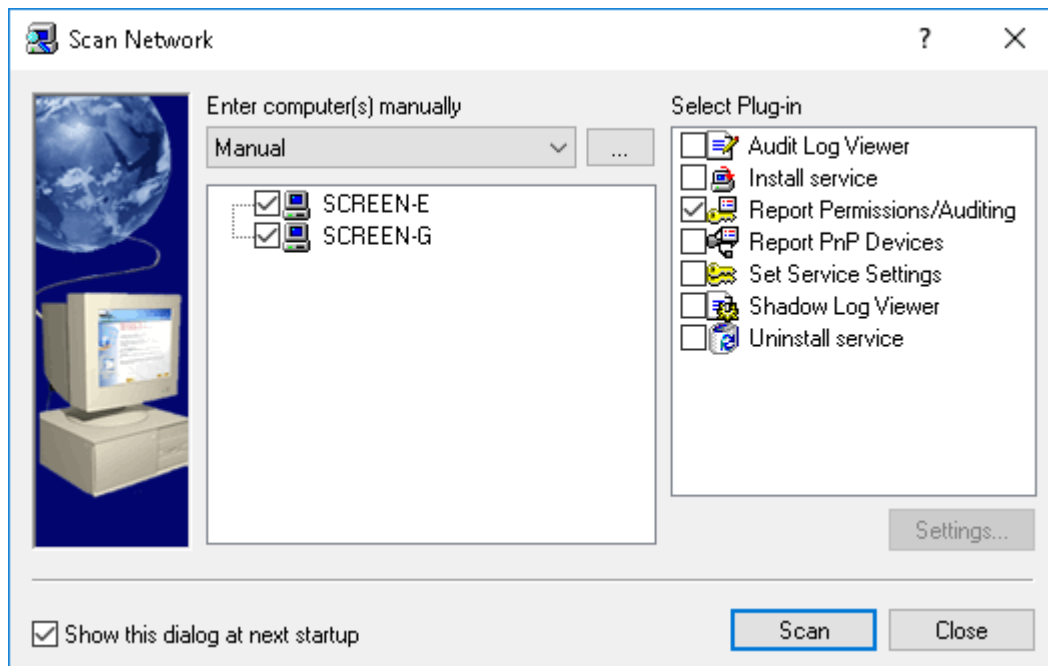
There is a log window at the bottom of the main window. The log window is used to display useful information about ongoing activity as well as diagnostic and error messages. There are two log lists: **Information** and **Warnings/Errors**.



You can click the right mouse button on the log window to open the useful shortcut menu.

## Scan Network Dialog Box

The **Scan Network** dialog box allows you to select computers on your network and the action (install or remove DeviceLock Service, set permissions, and so on) which should be performed for these computers.



To open the **Scan Network** dialog box, click **Scan Network** on the **File** menu or click the appropriate button on the main toolbar. If the **Show this dialog at next startup** check box is selected, the **Scan Network** dialog box will open automatically each time DeviceLock Enterprise Manager is started.

There are three simple steps, which enable you to manage DeviceLock Services across the network.

## Selecting Computers

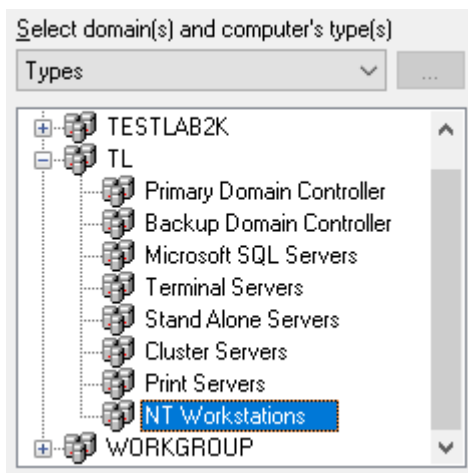
The first step is to select the computers to be processed. You can use the shortcut menu, available by right clicking, to select/deselect necessary items (computers types, domains, or computers).

DeviceLock Enterprise Manager provides several flexible ways to select network computers.

- Network computers can be selected by their types. Each type represents all of the computers belonging to the category:
  - Primary Domain Controller - A primary domain controller.
  - Backup Domain Controller - A backup domain controller.
  - Microsoft SQL Servers - Any server running with Microsoft SQL Server.
  - Terminal Servers - Any server where Terminal Services are running.
  - Stand Alone Servers - Any server that is not a domain controller.
  - Cluster Servers - Server clusters available in the domain.
  - Print Servers - Any computer that is sharing the print queue.
  - NT Workstations - Any computer running Windows XP/Vista/7/8/10 or Windows Server 2003/2008/2012/2016/2019.

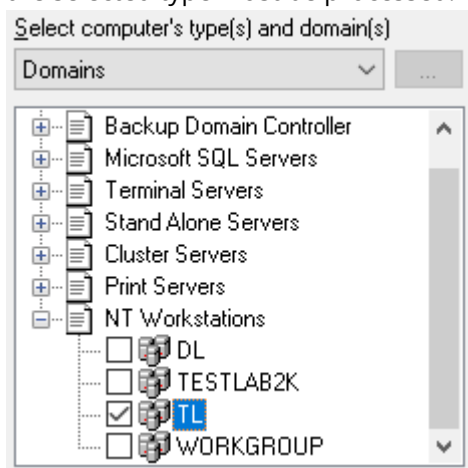
There are two ways to choose the type of computers:

1. **Types** - Select the network domain and then select types of computers which must be processed in this domain.



2. **Domains** - Select the type of computer and then select network domains where computers of

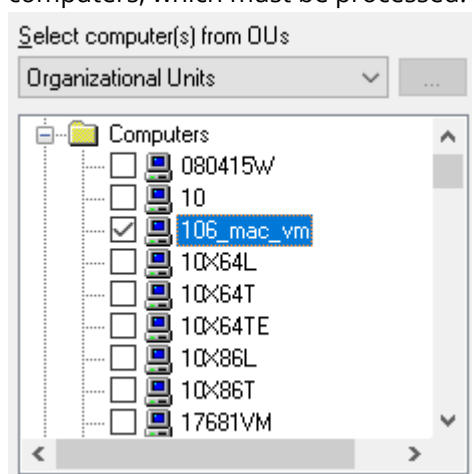
the selected type must be processed.



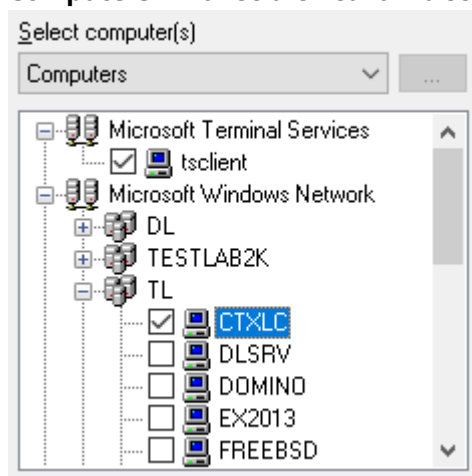
- Network computers can also be selected by their names.

There are several ways to choose computers by name:

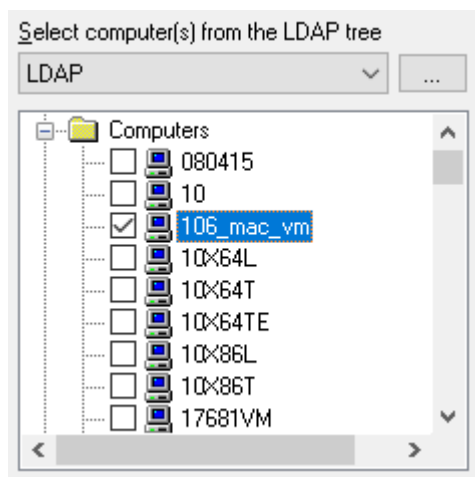
1. **Organizational Units** - Browse Active Directory organizational units (OUs) and select computers, which must be processed.



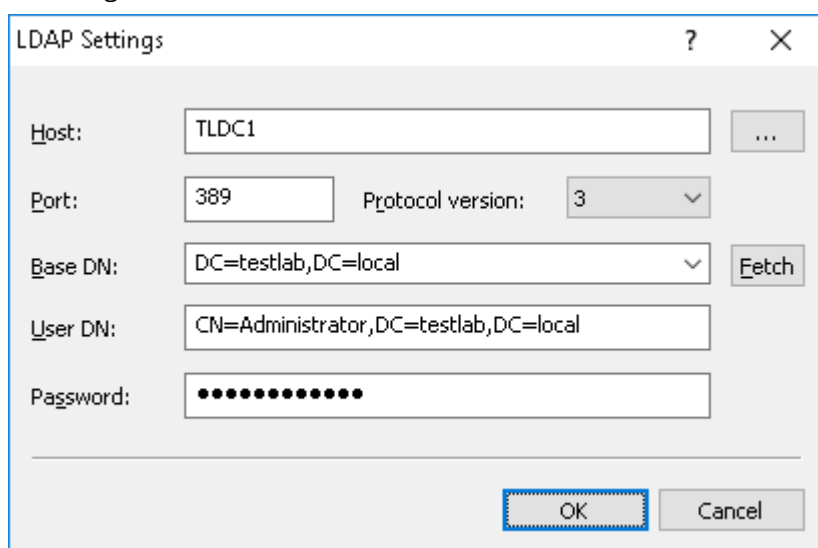
2. **Computers** - Browse the network tree and select computers.



3. **LDAP** - Browse the LDAP (Lightweight Directory Access Protocol) tree and select computers from the directory.



To configure a connection to the LDAP server, click the **...** button.

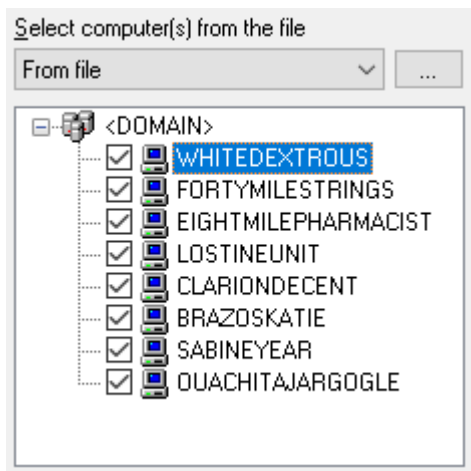


Complete the **LDAP Settings** dialog box that appears:

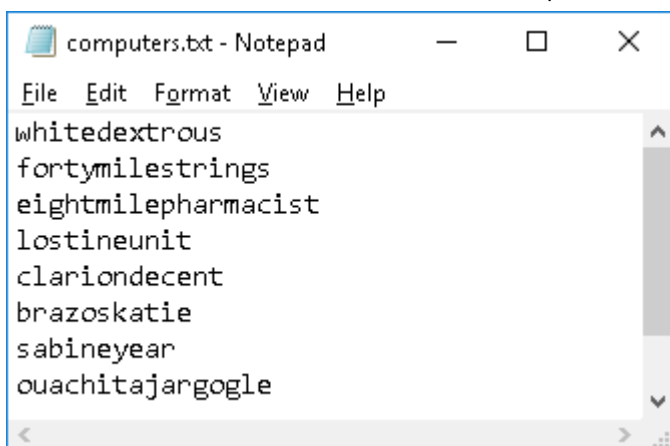
- **Host** - The name or the IP address of the LDAP server to connect to.
- **Port** - The TCP port on which the LDAP server accepts connections. The default port is 389.
- **Protocol version** - The LDAP protocol version. Some servers are not fully compatible with the LDAP v.3 protocol and LDAP requests require certain adjustments for correct communication with such servers. Selecting **Version 2** makes sure that the server requests are adjusted according to the LDAP v.2 protocol requirements.
- **Base DN** - The starting point to search the directory tree. You must use the LDAP string representation for distinguished names (for example, cn=users,o=company,c=US). Leave the **Base DN** box blank to search the directory tree from the root.  
By clicking the **Fetch** button, you can get all the published naming contexts to choose the base DN from.
- **User DN** - The distinguished name (DN) of the directory user that allows connection to the directory. You must use the LDAP string representation for distinguished names (for example, cn=admin,o=company,c=US).
- **Password** - The user's password.

4. **From File** - Load a predefined list of computers from the external text file and then select the computers.

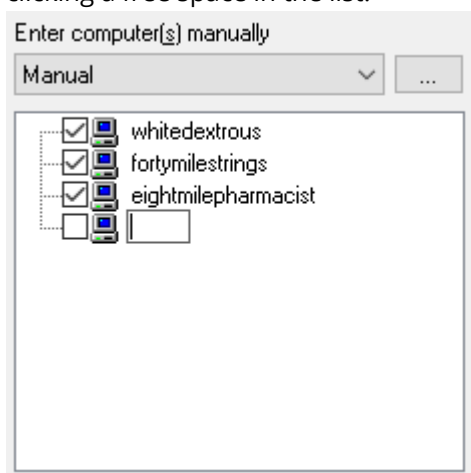
To open an external file, click the **...** button.



A text file must contain each computer's name or IP address on separate lines and can be either Unicode or non-Unicode. A brief example of such a file follows:



5. **Manual** - Add entries to the list of computers by hand, type a computer name or IP address in each entry, and then select the computers. Save the entry by pressing the ENTER key or by clicking a free space in the list.

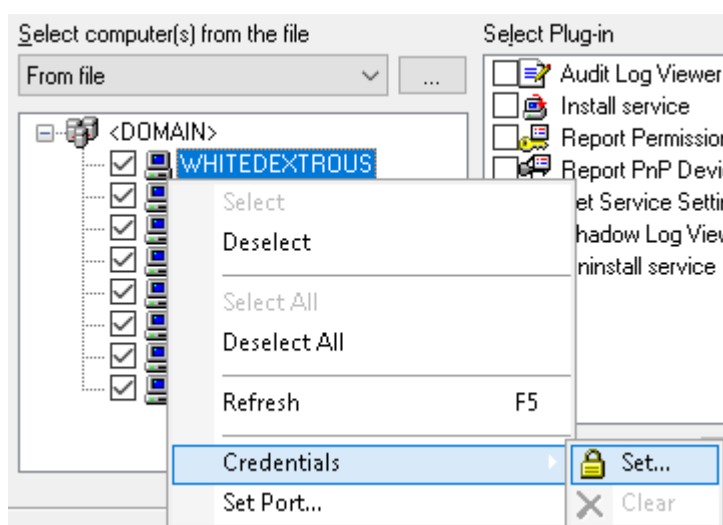


To add an entry to the list of computers, do either of the following:

- Double-click a free space in the list.
- Right-click a free space in the list, and then click **Add** on the shortcut menu.
- Click a free space in the list, and then press either the INSERT key or the PLUS (+) key on the numeric keypad.
- Click the **...** button to select computers using the dialog box provided by the operating system.

## Supplying Credentials

If you need to supply alternative credentials for the target computer(s), select the computer or network domain from the tree and point to **Credentials** on the shortcut menu.

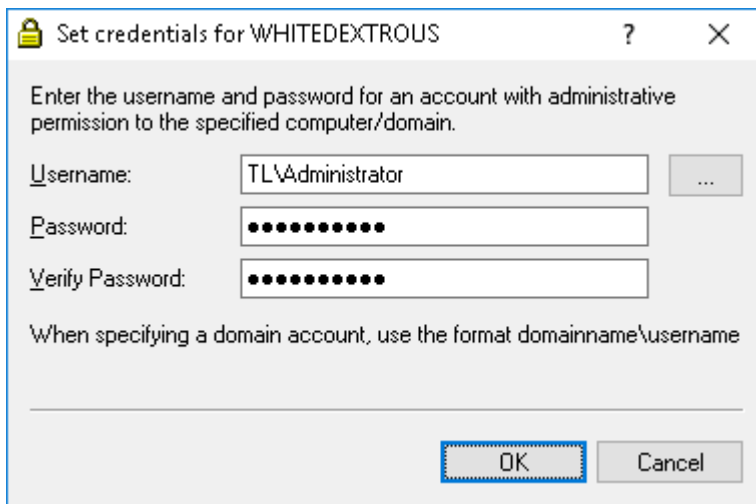


You may assign credentials to individual computers and/or to network domains. To add credentials, click **Set**. To delete alternative credentials, click **Clear**.

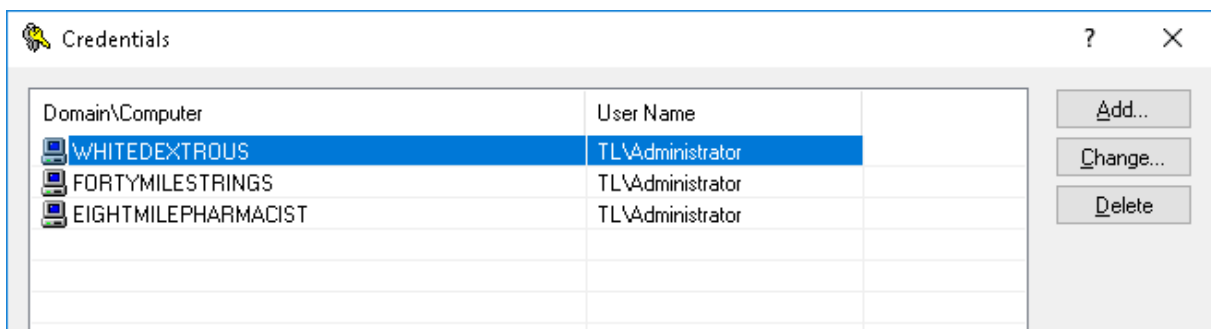
Credentials consist of a user name and password pair used to authenticate the computers processed. By default, DeviceLock Enterprise Manager uses your currently logged on credentials to automatically log in and process the target computer(s). If the current logged-in user credentials do not have administrative rights on all of the target computers, you need to enter alternate credentials. DeviceLock Enterprise Manager will use these alternate credentials to automatically login to the target computers.

In all cases, credentials are stored with encryption techniques and are not available to anyone except the user with administrative privileges.





Credentials can also be supplied via the **Credentials** dialog box. To open the **Credentials** dialog box, click **Credentials** on the **File** menu.

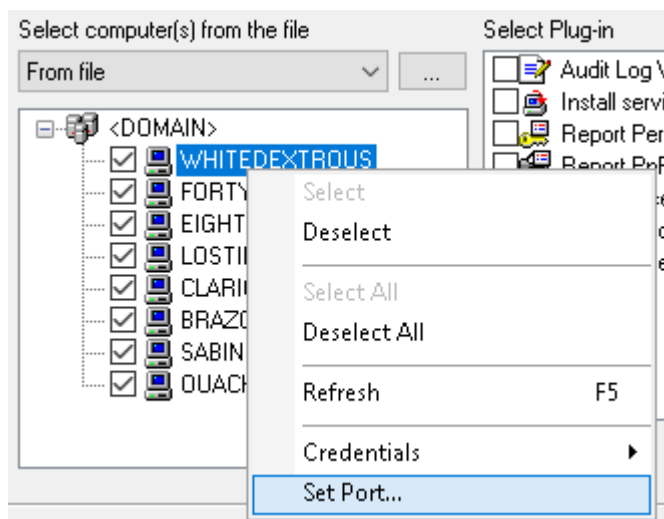


Click **Add** to add new credentials. To change existing credentials, select the record in the list and click **Change**.

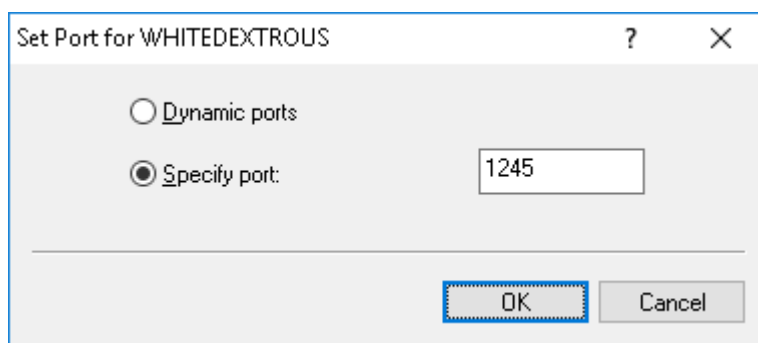
To delete credentials, select the record in the list and click **Delete**. Using CTRL and/or SHIFT you can select and remove several records simultaneously.

## Setting Port

You can instruct DeviceLock Enterprise Manager to use a fixed port, making it easier to configure a firewall. To do so, use **Set Port** from the shortcut menu.



By default, DeviceLock Enterprise Manager uses dynamic ports for RPC communication with DeviceLock Service. However, if DeviceLock Service is configured to accept connections on a fixed port, select the **Specify port** option.



To use the dynamic ports binding, click **Dynamic ports**.

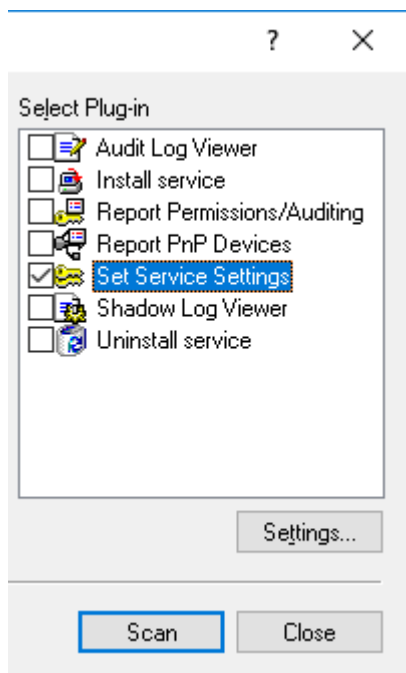
DeviceLock Service can be configured to use either a fixed port or dynamic ports during the installation process. For more information on this, see [Unattended Installation](#) and [Installation via DeviceLock Enterprise Manager](#).

If you need to change the port configuration when DeviceLock Service is already installed, use the [Install Service](#) plug-in.

For information on which ports are required for which actions, refer to the [Plug-ins](#) section of this manual.

## Selecting Plug-ins

The second step is to select a plug-in to process the network computers selected on the first step. To select/deselect plug-ins, you can use the shortcut menu available with a right mouse click.



To define parameters for the selected plug-in, use the **Settings** button below the plug-ins list. If the plug-in does not have additional parameters, this button is unavailable.

Tasks are passed to the plug-in by DeviceLock Enterprise Manager.

The plug-in performs the task and returns the information to DeviceLock Enterprise Manager. Upon receipt of a plug-in's information, DeviceLock Enterprise Manager displays it in a separate window.

## Starting a Scan

Once you have selected computers and the appropriate plug-in, the final step is starting the scan process. Click **Scan** to initiate the process.

Right after the scan process is initiated, you can start to explore the information that is already received from the plug-in.

Because the scan process runs in a separate thread, you do not need to wait until all computers are finished being scanned. You can also perform other tasks in the DeviceLock Enterprise Manager interface.

There are only a few things which you cannot do while the scan is running - you cannot close DeviceLock Enterprise Manager and you cannot run another scan process.

If, for some reason, you wish to abort the active scan process, you can click **Stop Scan** on the **File** menu or click the appropriate button on the main toolbar.



The scan process will be aborted as soon as a plug-in returns control to DeviceLock Enterprise Manager.

## Plug-ins

DeviceLock Enterprise Manager has a flexible plug-in based architecture that allows you to plug in the necessary module on demand. DeviceLock Enterprise Manager loads the plug-ins on startup from the `Plugins` folder, located in the main DeviceLock Enterprise Manager directory.

DeviceLock Enterprise Manager ships with standard plug-ins that require some network ports to be opened on remote computers, as described in the table below:

Required ports	Plug-ins affected
<b>TCP 139 or TCP 445</b> <b>UDP 137</b> - This port must be opened only when a connection is established by the computer name. If an IP address is used, this port is not required.	<a href="#">Audit Log Viewer</a> <a href="#">Report PnP Devices</a>
<b>TCP 139 or TCP 445</b> <b>UDP 137</b> - This port must be opened only when a connection is established by the computer name. If an IP address is used, this port is not required.	<a href="#">Install Service</a> <a href="#">Uninstall Service</a>
<b>TCP 139 or TCP 445</b> <b>TCP 135</b> - This port is required only when the <b>Dynamic ports</b> connection is used. <b>TCP &lt;all ports above 1024&gt;</b> - These ports are required only when the <b>Dynamic ports</b> connection is used. <b>TCP &lt;custom port&gt;</b> - This port is required only when the <b>Fixed port</b> connection is used. <b>UDP 137</b> - This port must be opened only when a connection is established by computer name. If an IP address is used, this port is not required.	<a href="#">Report Permissions/Auditing</a> <a href="#">Set Service Settings</a> <a href="#">Shadow Log Viewer</a>

For information on how to use either the **Dynamic ports** or **Fixed port** connection in DeviceLock Enterprise Manager, see [Setting Port](#).

When a plug-in is connected to a remote computer it may receive some of these error messages:

- **The product version on the client and server machines does not match (7049)** - You are trying to connect to a computer where an old version of DeviceLock Service is installed. You should upgrade DeviceLock Service first using the [Install Service](#) plug-in.
- **The network path was not found (53)** - You are trying to connect to a computer that either does not exist (the wrong name or IP address) or is not accessible. Make sure that the computer name you have specified is correct. Try to access this computer with Windows Explorer and connect to it using any standard Windows administrative tool (such as Computer Management, Services and so on).

*This error also occurs when the standard Windows Server service is not running on the remote computer. Check the Server service status and start it if it is stopped.*

More connection errors are described in the [Possible connection errors](#) section of this manual.

From a report produced by any plug-in, you can open DeviceLock Management Console connected to DeviceLock Service on a given computer: right-click the computer name, and then click **Connect to DeviceLock Service**.

## Audit Log Viewer

The Audit Log Viewer plug-in retrieves DeviceLock's audit log from the computer's local Windows event logging subsystem.

To define a maximum log size and what Windows should do if the audit log becomes full, use **Audit Log Settings** from the shortcut menu. To clear all events from the audit log, select **Clear Audit Log** from the shortcut menu.

For more information, see [Audit Log Viewer \(Service\)](#).

## Install Service

The Install Service plug-in installs or updates DeviceLock Service on computers.

---

### Note

Only the built-in administrator account can be used to perform a remote installation of DeviceLock Service on computers running Windows Vista or a later version of Windows. In a Windows Active Directory environment, only members of the Domain Admins group can perform a remote installation of DeviceLock Service. Administrator privileges are required to connect to DeviceLock Service via DeviceLock Management Console. For more information, refer to Microsoft's article at [support.microsoft.com/kb/951016](https://support.microsoft.com/kb/951016).

---

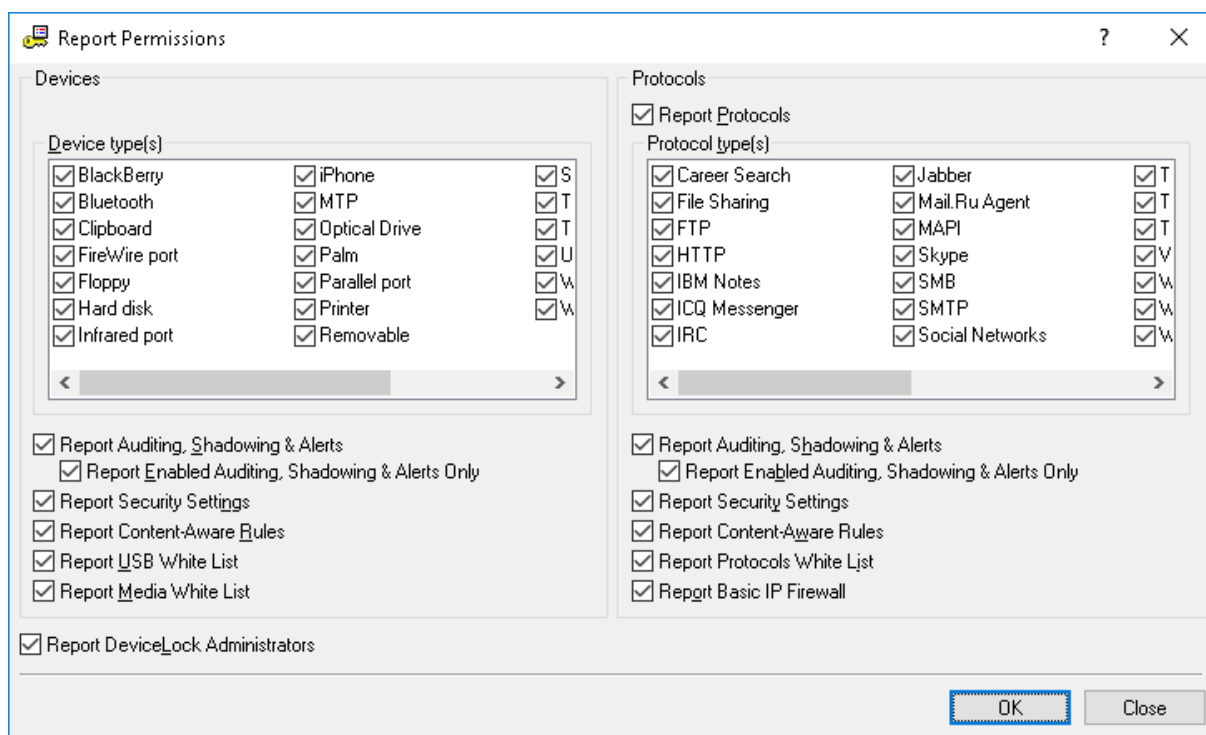
Before you can use this plug-in, you should specify the directory that contains all of the files needed for installation (such as DeviceLock Service.msi, DeviceLock Service x64.msi, DLRemoteInstaller.exe, and InstMsiW.exe). You can do this by clicking the **Settings** button below the plug-ins list in the **Scan Network** dialog box (see [Selecting Plug-ins](#)).

For more information, see [Installation via DeviceLock Enterprise Manager](#).

## Report Permissions/Auditing

The Report Permissions/Auditing plug-in generates a report that allows you to view and change security policies defined for device types and protocols across the network.

Before you can use this plug-in, you should select the information you want to include in the report, by clicking the **Settings** button below the plug-ins list in the **Scan Network** dialog box (see [Selecting Plug-ins](#)).



In the **Report Permissions** dialog box that appears when you click the **Settings** button, specify the information that you want to include in your report.

To receive information on the security policies defined for device types, under **Devices**, use the following options:

- **Report Auditing, Shadowing & Alerts** - Select this check box to report audit, shadowing rules and alerts that have been set. Also when this check box is selected, you receive information about whether the [Log Policy changes and Start/Stop events](#) parameter is enabled in [Service Options](#).
- **Report Enabled Auditing, Shadowing & Alerts Only** - Select this check box to exclude devices for which audit, shadowing rules and alerts are disabled from the report.  
*This option is available only if the Report Auditing, Shadowing & Alerts check box is selected.*
- **Report Security Settings** - Select this check box to report what parameters are disabled via Security Settings (see [Security Settings \(Regular Profile\)](#)).
- **Report Content-Aware Rules** - Select this check box to report Content-Aware Rules that have been set (see [Rules for Devices in Content-Aware Rules \(Regular Profile\)](#)).
- **Report USB White List** - Select this check box to include information about white listed devices (see [USB Devices White List \(Regular Profile\)](#)).
- **Report Media White List** - Select this check box to include information about white listed media (see [Media White List \(Regular Profile\)](#)).
- **Report DeviceLock Administrators** - Select this check box to report accounts that can manage DeviceLock Service or view its settings and logs.

To receive information on the security policies defined for protocols, under **Protocols**, use the following options:

- **Report Protocols** - Select this check box to report security policies for protocols. Otherwise, information on all protocol-based policies will be excluded from the report.  
*If the Report Protocols check box is cleared, the Report Auditing, Shadowing & Alerts option and the Report Enabled Auditing, Shadowing & Alerts Only option are unavailable.*
- **Report Auditing, Shadowing & Alerts** - Select this check box to report audit, shadowing rules and alerts that have been set for protocols.
- **Report Enabled Auditing, Shadowing & Alerts Only** - Select this check box to exclude protocols for which audit, shadowing rules and alerts are disabled from the report.  
*This option is available only if the Report Auditing, Shadowing & Alerts check box is selected.*
- **Report Security Settings** - Select this check box to report what parameters are defined via Security Settings (see [Managing Security Settings for Protocols](#)).
- **Report Content-Aware Rules** - Select this check box to report Content-Aware Rules that are set for protocols (see [Rules for Protocols](#) in [Content-Aware Rules \(Regular Profile\)](#)).
- **Report Protocols White List** - Select this check box to include information about white listed protocols (see [Managing Protocols White List](#)).
- **Report Basic IP Firewall** - Select this check box to report Basic IP Firewall rules that have been set (see [Managing Basic IP Firewall](#)).

This report always includes information about an installed DeviceLock Certificate (see [DeviceLock Certificates](#)). Also, it always shows whether the [Use Group/Server Policy](#) parameter is enabled in [Service Options](#).

## Report PnP Devices

The Report PnP Devices plug-in generates a report displaying the USB, FireWire and PCMCIA devices currently connected to computers on the network and those that were connected.

---

### Note

- In order to retrieve PnP devices from computers running Windows 8/10 or Windows Server 2012/2016/2019, you should install DeviceLock Service on those computers.
  - In order to retrieve PnP devices from computers running Windows Vista/7 or Windows Server 2008, you should allow remote access to the PnP interface on those computers. You can do it by modifying the policy as described in our article at [www.device-lock.com/support/kb\\_view.html?ID=14800](http://www.device-lock.com/support/kb_view.html?ID=14800) (see the title "Enable Remote Access to the Plug and Play (PNP) Interface" there).
- 

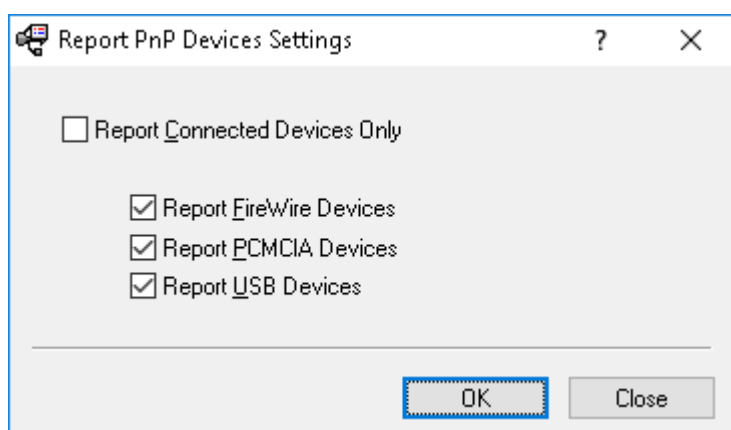
The columns are defined as follows:

- **Description** - The device description provided by the device's vendor.
- **Device Information** - Additional information about the device provided by its vendor.
- **Connected to** - The interface where the device is connected (USB, FireWire or PCMCIA).
- **Class** - The class of the device provided by Windows.
- **Class description** - A description of the device's class provided by Windows.
- **Present** - Indicates whether the device is currently connected or not (**Yes** or **No**).

- **DeviceID** - The unique identification string of the device provided by its vendor.
- **Driver** - The Name of the driver that is controlling this device.

You can add reported USB devices to the [USB Devices Database](#) using the shortcut menu available via a right mouse click.

Before you can use this plug-in, you should select the information you want to include in reports, by clicking the **Settings** button below the plug-ins list in the **Scan Network** dialog box (see [Selecting Plug-ins](#)).



- **Report Connected Devices Only** - Select this check box to report only those devices that are currently connected to the computer. Otherwise, you will see all devices that were ever connected to the computer.
- **Report FireWire Devices** - Select this check box to report devices that are plugging into the FireWire port.
- **Report PCMCIA Devices** - Select this check box to report devices that are plugging into the PCMCIA slot.
- **Report USB Devices** - Select this check box to report devices that are plugging into the USB port.

## Set Service Settings

The Set Service Setting plug-in reads the policy (settings, permissions, audit, shadowing rules and alerts) from the settings file and deploys it to DeviceLock Services across the network.

---

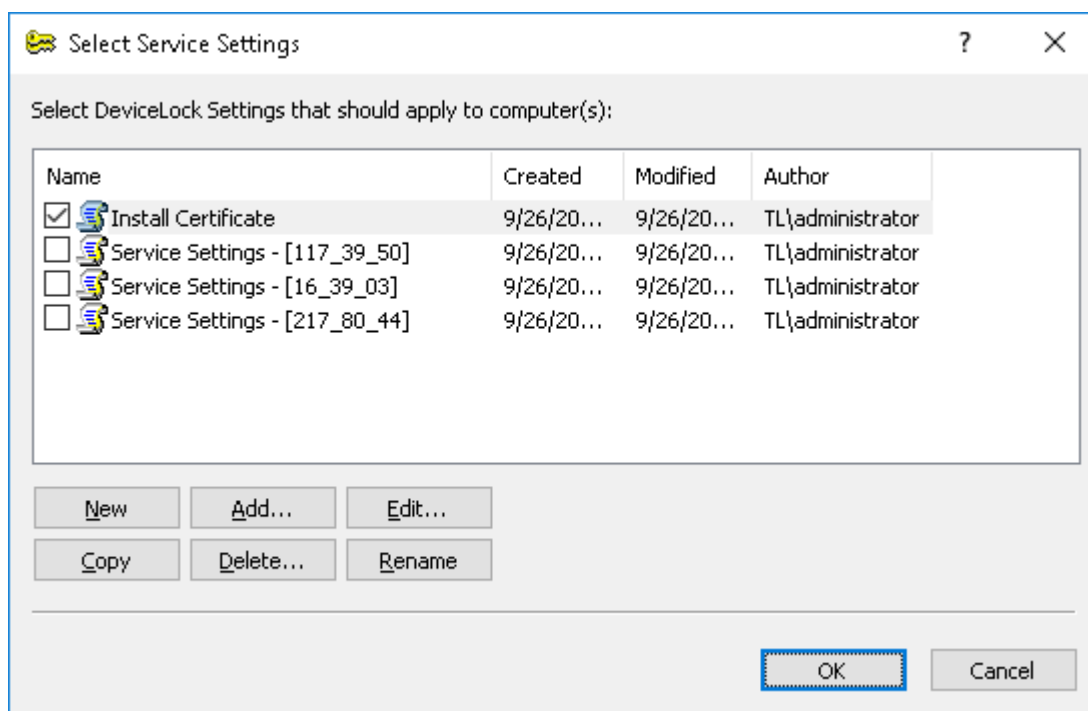
### Note

Only settings that are explicitly defined in a policy file apply to client computers. All policy settings that have the **Not Configured** state are ignored by client computers.

---

Before you can use this plug-in, you should define settings, permissions and/or audit rules that you want to deploy. You can do this by clicking the **Settings** button below the plug-ins list in the **Scan Network** dialog box (see [Selecting Plug-ins](#)).





First of all you have to prepare the policy you want to deploy.

If there are no files in the list, then you can either create an empty file by clicking the **New** button or add an existing file by clicking the **Add** button.

Then select the file in the list and click **Edit** to open DeviceLock Service Settings Editor. DeviceLock Service Settings Editor is used for creating and modifying files with settings, permissions, audit, shadowing rules and alerts for DeviceLock Service (DeviceLock Service settings files). For more information, see [DeviceLock Service Settings Editor](#).

When finished modifying the policy, select its file by selecting the check box next to the file's name in the list. Then click **OK** to close the configuration dialog box.

## Shadow Log Viewer

The Shadow Log Viewer plug-in retrieves the shadow log from DeviceLock Service.

Use the shortcut menu available by a right mouse click to access all this plug-in's functions.

For more information, see [Shadow Log Viewer \(Service\)](#).

## Uninstall Service

The Uninstall Service plug-in removes DeviceLock Service and all its settings and components from computers.

If the user under which DeviceLock Enterprise Manager is connecting to the computer does not have full administrative access to DeviceLock Service, the plug-in will not be able to remove the service.

Likewise, an error occurs when the user does not have local administrative privileges on the computer where DeviceLock Service is running.

## Open / Save / Export

DeviceLock Enterprise Manager can store all information received from plug-ins.

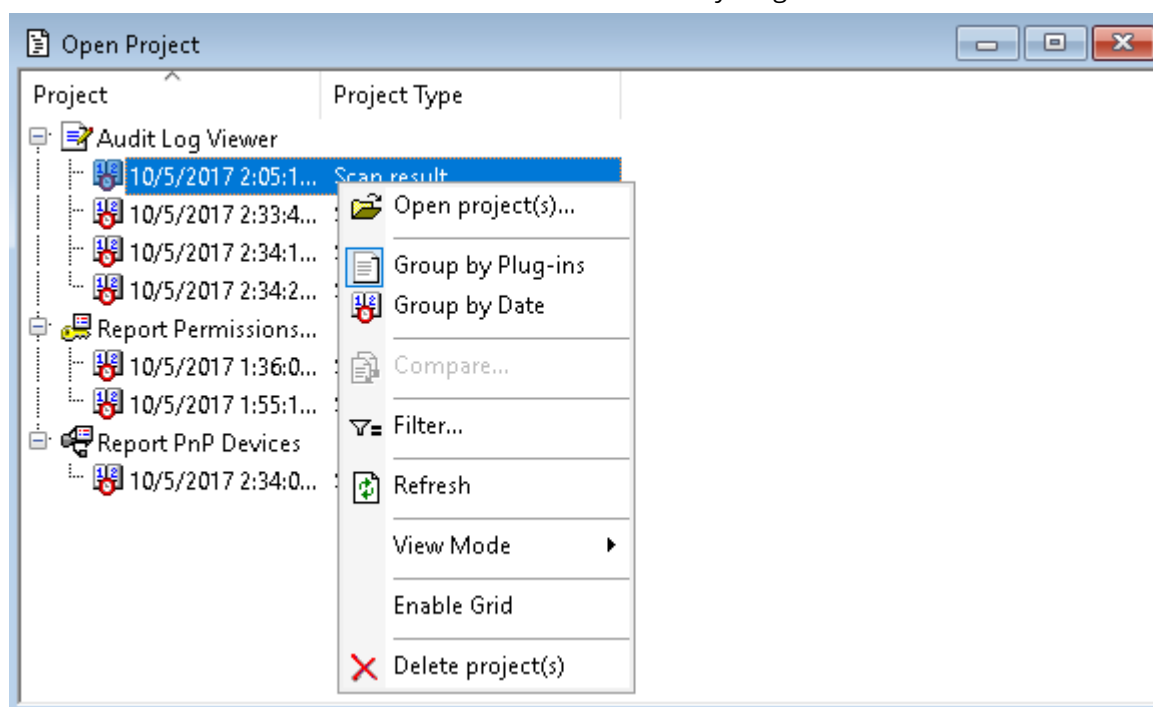
The data is saved to external files and is ready for loading into DeviceLock Enterprise Manager when requested.

There are three ways to save and load data:

1. The handiest method to store received information is to save it as a project. When you are saving data as a project, DeviceLock Enterprise Manager saves each active plug-in's window to a separate file of its own format and places this file in the **Project** subdirectory. The names of the project's files are auto-generated and depend on the plug-in's names and the date and time when the scan was started.

To save the data as a project, you can select **Save Project** from the **File** menu or click the appropriate button on the main toolbar.

To load previously saved projects, select **Open Project** from the **File** menu. The **Open Project** window has its own toolbar and shortcut menu available by a right mouse click.



You can group saved projects by the date when they were scanned and by the type of information they contain. Select **Group by Plug-ins** or **Group by Date** from the shortcut menu or click appropriate buttons on the **Project** toolbar.

To open a saved project, select it from the list and click the **Open Project** button on the **Project** toolbar. Using CTRL and/or SHIFT, you can select and open several projects simultaneously.

2. Another way to save received information in the format of DeviceLock Enterprise Manager is select **Save As** from the **File** menu. This enables you to save a file of the ANM type to any place on your hard disk or any other media with any name you choose.  
To load previously saved files, you can select **Open** from the **File** menu or click the appropriate button on the main toolbar. You will need to specify a file you wish to open. You can load files of the ANM type only.
3. If you need to pass received information to a third-party application, you can export it into an external file and then import it to this application. To export data into the external file, select **Save As** from the **File** menu and then select the file's type from the **Save as type** box.  
DeviceLock Enterprise Manager supports the export into MS Excel (if it is installed on the local computer) and two formats of text files - Tab Delimited (TXT) and Comma Delimited (CSV).  
If you export information into an external file, you will not be able to load it back to DeviceLock Enterprise Manager because DeviceLock Enterprise Manager can open and load only files of its own format. However, the ability to export into an external file is useful when you wish to exchange data between DeviceLock Enterprise Manager and other applications.

## Comparing Data

DeviceLock Enterprise Manager allows you to track changes on network computers by comparing two previously saved projects. Tracking changes is important when managing a wide range of computers on one network.

DeviceLock Enterprise Manager provides a very useful and intuitive Wizard to compare two ANM files. To open this Wizard, select **Compare** from the **File** menu.

There are three simple steps, which enable you to compare two files using the Compare Wizard:

1. The first step is to select the files you want to compare.

Select Projects To Compare

First file

:Lock\Projects\Report Permissions\_Auditing - [03\_10\_17 16\_59\_36].anm ...

Type Report Permissions/Auditing

Date 03.10.17 16:59:36

Second file

:Lock\Projects\Report Permissions\_Auditing - [04\_10\_17 11\_31\_43].anm ...

Type Report Permissions/Auditing

Date 04.10.17 11:31:43

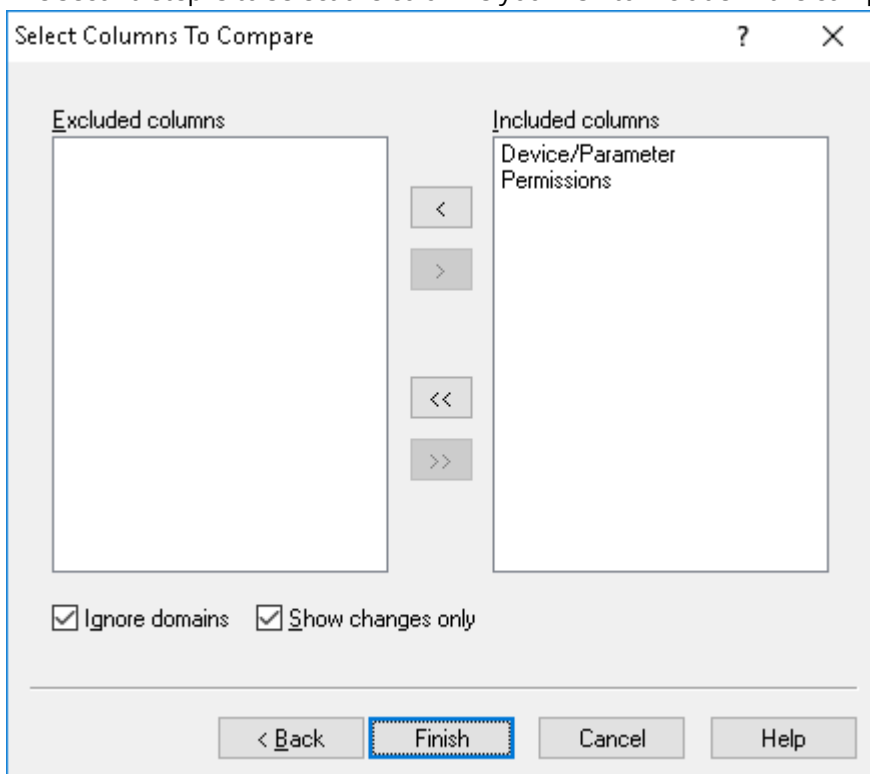
< Back Next > Cancel Help

Select the first file and then select the second file by using the ... buttons.

Please note that you can compare files of the same type only. For example, you cannot compare information received from the Report Permissions/Auditing plug-in with information from the Report PnP Devices plug-in.

When you have selected two files, click the **Next** button to go to the Wizard's next page.

2. The second step is to select the columns you wish to include in the compare process.



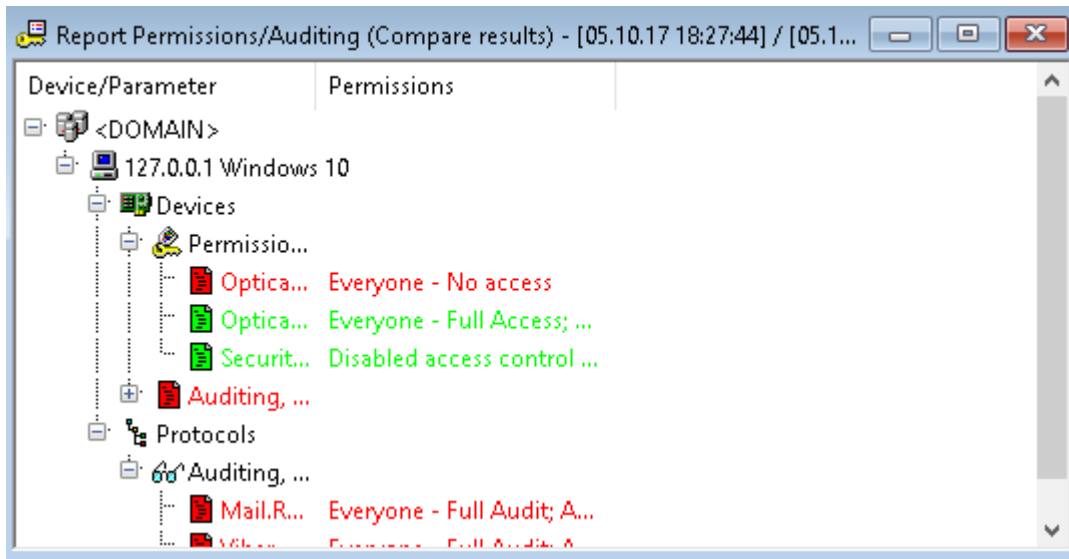
DeviceLock Enterprise Manager compares only those columns, which you have selected. If you need to exclude one column from the compare process, you have to move it from the **Included columns** list to the **Excluded columns** list. Excluded columns will be visible in the compare result, but the values they contain are ignored and do not affect the compare result.

By default, the compare result contains only records, which are different in the two files being compared. If you would like to see all of the records (even unchanged records), you can clear the **Show changes only** check box.

To include names of the network domains in the compare process, you can clear the **Ignore domains** check box. When the **Ignore domains** check box is selected, DeviceLock Enterprise Manager ignores domains and only compares computers and the information those computers contain.

3. The third and final step is to start the compare process. Click the **Finish** button to compare two selected files with each other.

*DeviceLock Enterprise Manager displays the compare result in a separate window in the form of a tree exactly as it displays information received from a plug-in.*



The comparison is very simple and effective:

1. If the **Ignore domains** check box is cleared, the program enumerates network domains in the two selected files and tries to find each domain in both the older file and the recent file.  
If the domain exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing domain (along with all the computers contained in that domain as well as the information in those computers) into the comparison result and then writes all those records in red.  
If the domain does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing domain (along with all the computers contained in that domain as well as the information in those computers) into the comparison result and then writes all those records in green.  
If the domain exists in both files, DeviceLock Enterprise Manager enumerates all the computers the domain contains (see below).
2. If the **Ignore domains** check box is selected, DeviceLock Enterprise Manager ignores domains and enumerates all the computers in the two selected files and tries to find each computer in both older and recent files.  
If the computer exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing computer with all information it contains into the compare result and writes all these records in red.  
If the computer does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing computer with all information it contains into the compare result and writes all these records in green.  
If the computer exists in both files, DeviceLock Enterprise Manager enumerates all the information it contains (see below).
3. DeviceLock Enterprise Manager enumerates all information for a computer and tries to find each record in both the older and the recent file.  
If the record exists in the older file but does not exist in the recent file, DeviceLock Enterprise Manager inserts the missing record into the compare result and writes it in red.

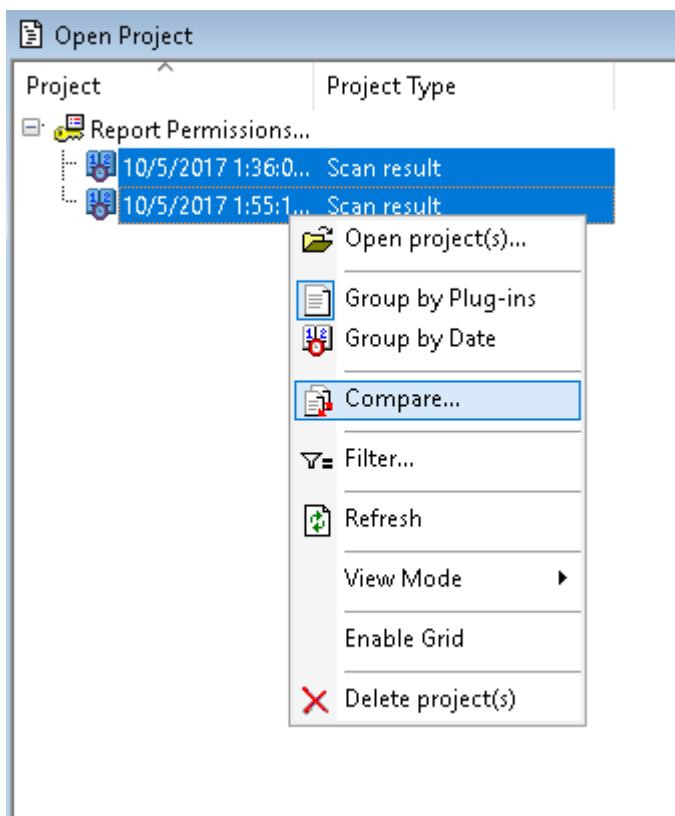
If the record does not exist in the older file but exists in the recent file, DeviceLock Enterprise Manager inserts the missing record into the compare result and writes it in green.

If the record exists in both files, DeviceLock Enterprise Manager starts comparing each included column for this record:

- If the column's values for the older and the recent files are different, DeviceLock Enterprise Manager inserts both records in the compare result. The record from the recent file comes right after the record from the older one.  
*The column that belongs to an older record is highlighted in red. The column that belongs to a recent record is highlighted in green. All excluded columns and columns with equal values are not highlighted and are written in the default color.*
- If all of a record's columns for both files contain equal values, DeviceLock Enterprise Manager either skips this record (the **Show changes only** check box is selected) or inserts this record into the compare result and writes it in the default color (the **Show changes only** check box is cleared).

If you wish to compare two files, which were saved as projects, it is a good idea to use the special feature of the **Open Project** window.

Select **Open Project** from the **File** menu, select two projects you would like to compare (use CTRL and/or SHIFT to select two projects simultaneously) and then select **Compare** from the shortcut menu or click the appropriate button on the **Project** toolbar.



---

#### Note

You may select only two projects and both projects must be of the same type.

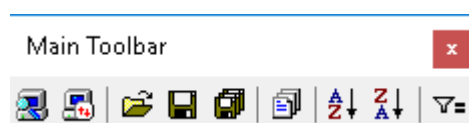
---

DeviceLock Enterprise Manager provides a toolbar to help you navigate through the comparison results:



Click the leftmost or middle button on the toolbar to go to the previous or next change in the comparison results. The rightmost button opens the legend of the comparison results display.

You can also save the compare result to an external ANM file or export it into MS Excel or the text file (TXT and CSV). Select **Save As** from the **File** menu or click the appropriate button on the main toolbar to save or export the compare result.

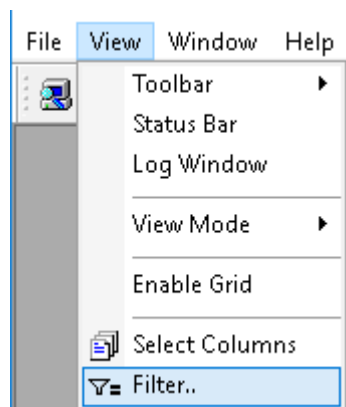


As with any other DeviceLock Enterprise Manager file, the saved compare result can be opened and loaded to DeviceLock Enterprise Manager. To load the previously saved compare result, you can select **Open** from the **File** menu or click the appropriate button on the main toolbar. You will need to specify a file you want to open. You can load files of ANM type only.

## Filtering Data

DeviceLock Enterprise Manager provides very sophisticated data filtering, enabling you to narrow a scan or comparison result to only those data complying to your specific conditions.

To open the **Filter Data** dialog box, you can select **Filter** from the **View** menu or click the appropriate button on the main toolbar.



---

### Note

The window with a scan or comparison result must be active to use data filtering.

---





If you want to narrow down the search to the string's exact case (so that "Explorer.exe" would be different from "explorer.exe"), select the **Match case (for string data)** check box. Otherwise, case is ignored ("Explorer.exe" is the same as "explorer.exe").

Logical operations that can be performed on non-string data:

- **Equal to (=)** - Selects data having field values that are identical to the defined value (for example, PID = 3764).
- **Greater than (>)** - Selects data having field values that are greater than the defined value (for example, PID > 4).
- **Less than (<)** - Selects data having field values that are less than the defined value (for example, PID < 4).
- **Not Equal to (!=)** - Selects data having field values that are different from the defined value (for example, PID != 0).
- **Between (in)** - Selects data having field values that are between the two defined values (for example, PID in 3000-4000).
- **Not Between (out)** - Selects data having field values that are outside of the two defined values (for example, PID out 3000-4000).
- **Regular expression** - Selects only data having field values matching an expression. The expression may contain wildcards (for example, 300\*).

If you do not want to perform a logical operation for a field, select **Not defined** from the list of logical operations.

- The **Value** columns contain user-defined arguments. The second **Value** column is used only when the **Between (in)** or **Not Between (out)** logical operation is selected. For all other logical operations only the first **Value** column is needed.

After you define a filtering expression, click the **Apply** button to start the filtering process.

You can save a filtered result in an external ANM file or export it to a text file (TXT and CSV) or MS Excel. Select **Save As** from the **File** menu or click the appropriate button on the main toolbar to save or export the filtered result.

As with any other DeviceLock Enterprise Manager file, filtered data can be opened and loaded into DeviceLock Enterprise Manager. To load a file, select **Open** from the **File** menu or click the appropriate button on the main toolbar. Then specify the file you want to open. You can only load files that were previously saved by DeviceLock Enterprise Manager.

## DeviceLock Certificates

DeviceLock Certificate is a cryptographic certificate that consists of two keys (a key pair) - private and public:

- The private key must be stored on the administrator's computer and only the administrator must be able to access it. Also, the private key may be installed on DeviceLock Enterprise Server and DeviceLock Content Security Server.

---

**Note**

Make sure that non-administrative users can't get access to the private key.

---

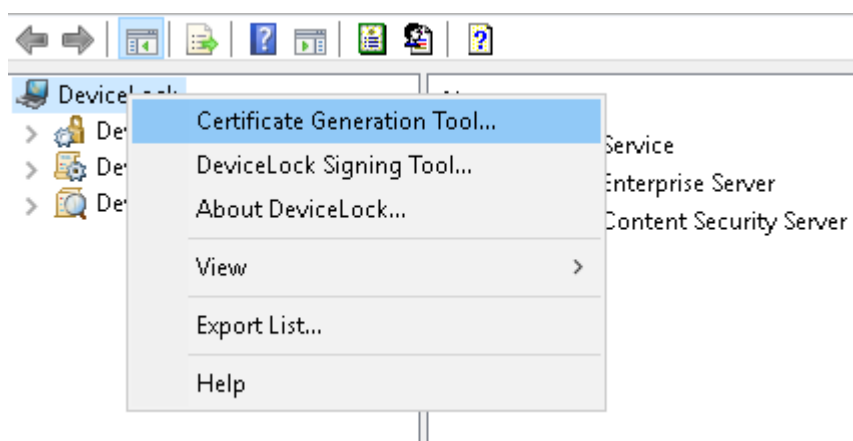
- The public key is installed on every computer where DeviceLock Service is running. If the public key has not been installed on the user's computer, there is no way to use [Temporary White List](#) function or DeviceLock Certificate-based authentication for DeviceLock Enterprise Server and DeviceLock Discovery.

## Generating DeviceLock Certificates

DeviceLock's Certificate Generation Tool allows you to generate DeviceLock Certificates.

We recommend that you generate only one DeviceLock Certificate and deploy its public key to all user computers. It is necessary to generate and install a new certificate only if the private key was either compromised (e.g. stolen) or lost.

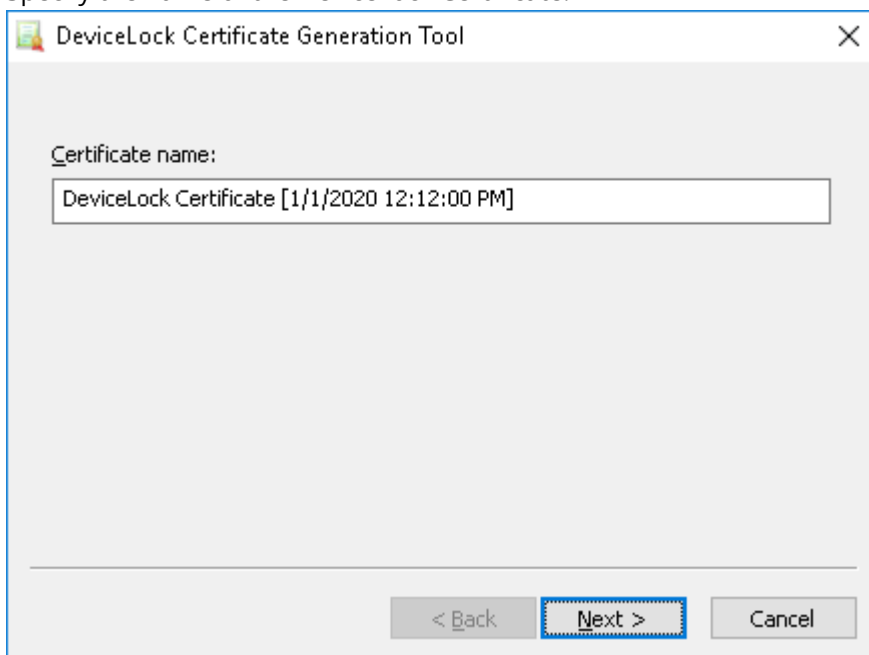
To run the Certificate Generation Tool, select the **Certificate Generation Tool** item from the **File** menu in DeviceLock Enterprise Manager. To run the Certificate Generation Tool from DeviceLock Management Console (the MMC snap-in) or DeviceLock Group Policy Manager, use the shortcut menu available by a right mouse click.



The Certificate Generation Tool starts automatically during installation of DeviceLock management consoles on an administrator's computer that has no DeviceLock Certificate.

There are two simple steps to generate the key pair:

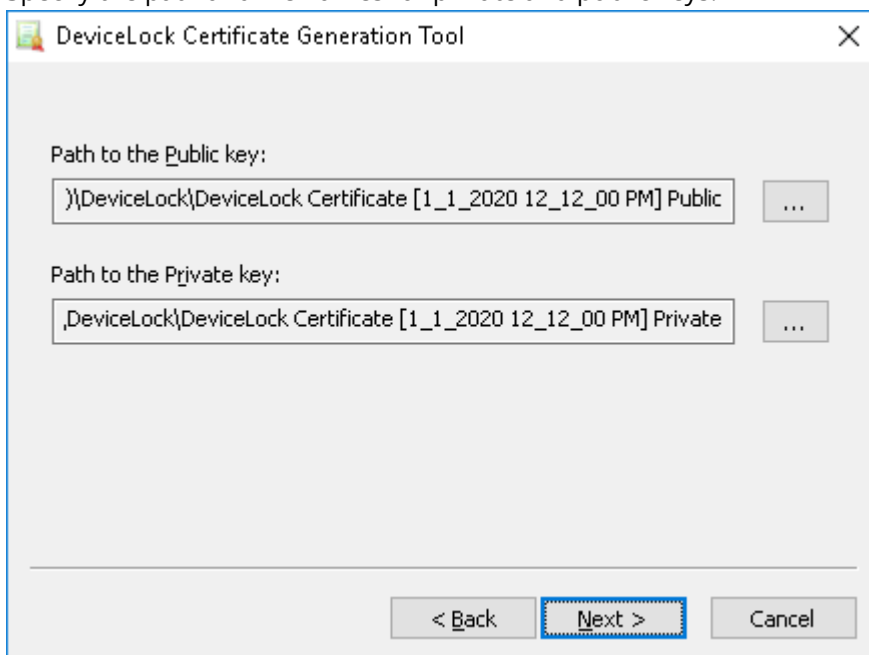
1. Specify the name of the DeviceLock Certificate.



The screenshot shows a Windows-style dialog box titled "DeviceLock Certificate Generation Tool". It has a close button (X) in the top right corner. The main area contains a label "Certificate name:" followed by a text input field. The input field contains the text "DeviceLock Certificate [1/1/2020 12:12:00 PM]". At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a blue dashed border), and "Cancel".

*The Certificate Generation Tool auto-generates a name based on the current date and time, but you can type any other name.*

2. Specify the path and file names for private and public keys.



The screenshot shows the same "DeviceLock Certificate Generation Tool" dialog box, now at Step 2. It contains two labels: "Path to the Public key:" and "Path to the Private key:". Each label is followed by a text input field and a browse button (three dots). The public key path field contains ".\\DeviceLock\\DeviceLock Certificate [1\_1\_2020 12\_12\_00 PM] Public" and the private key path field contains ".\\DeviceLock\\DeviceLock Certificate [1\_1\_2020 12\_12\_00 PM] Private". At the bottom, the "Next >" button is again highlighted with a blue dashed border.

Once the DeviceLock Certificate is created, the public key can be deployed to users' computers.

---

### **Important**

A newly generated DeviceLock Certificate does not automatically install on computers from the Certificate Generation Tool. You must deploy it manually from a DeviceLock management console.

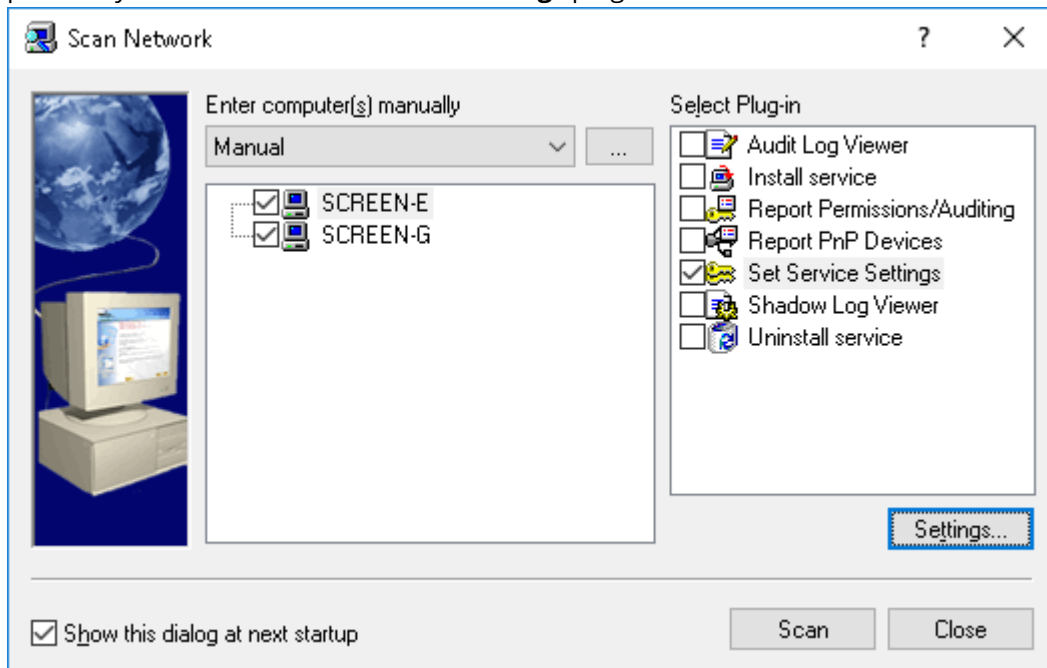
---

## Installing/Removing DeviceLock Certificate

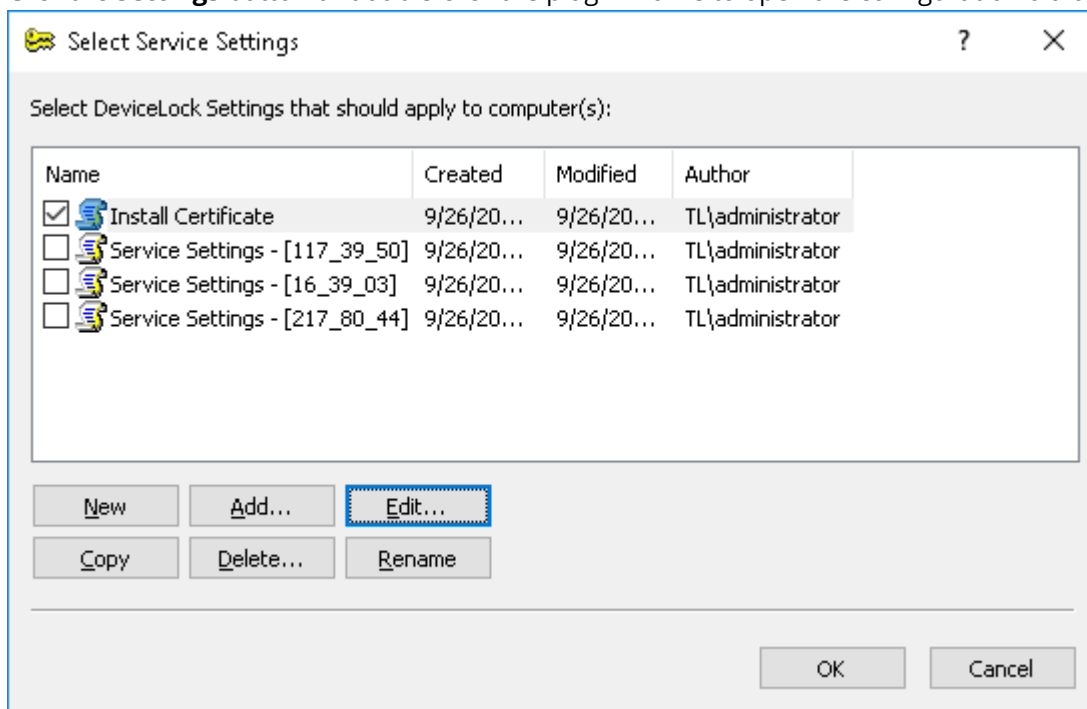
To install/remove the public key on/from user computers running DeviceLock Services, you can use any DeviceLock management console.

### Using DeviceLock Enterprise Manager

1. In the **Scan Network** dialog box, select the computers targeted for installation/removal of the public key and select the **Set Service Settings** plug-in.



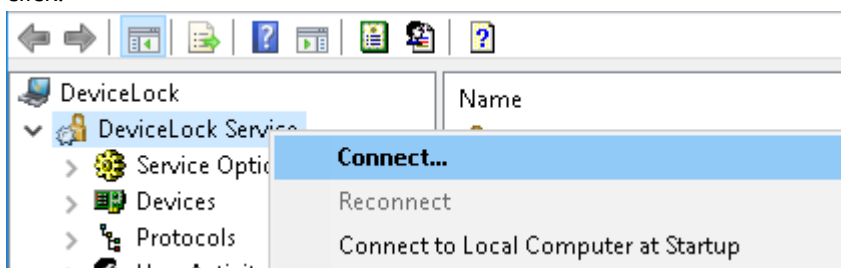
2. Click the **Settings** button or double-click the plug-in name to open the configuration dialog box.



3. Create the new DeviceLock Service settings file or use the existing one to define the policy needed to install/remove the certificate. Select the file in the list and then click the **Edit** button to modify the policy as described in the [Using DeviceLock Management Console, DeviceLock Group Policy Manager or DeviceLock Service Settings Editor](#) section later. When finished modifying the policy, select its file by selecting the check box next to the file's name in the list.
4. Click **OK** to close the configuration dialog box and then click the **Scan** button in the **Scan Network** dialog box to start the DeviceLock Certificate installation/removal process.

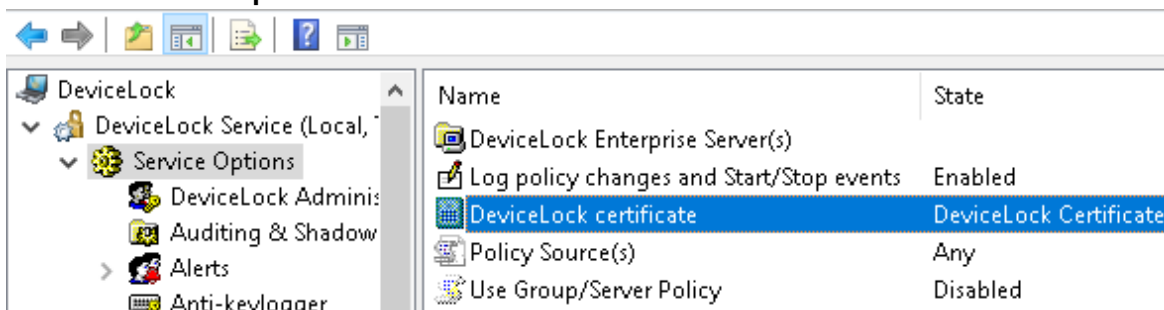
### ***Using DeviceLock Management Console, DeviceLock Group Policy Manager or DeviceLock Service Settings Editor***

1. If you are using DeviceLock Management Console (the MMC snap-in), first you need to connect it to the computer running DeviceLock Service. Use the shortcut menu available by a right mouse click.

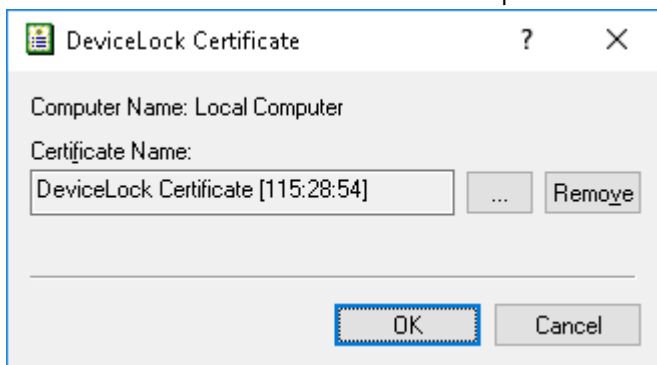


When DeviceLock Group Policy Manager is used, you don't need to connect to any computer since it connects to the Group Policy Object. Also, you don't need to connect to the computer when modifying the policy in the settings file using DeviceLock Service Settings Editor.

2. Select the **Service Options** item.



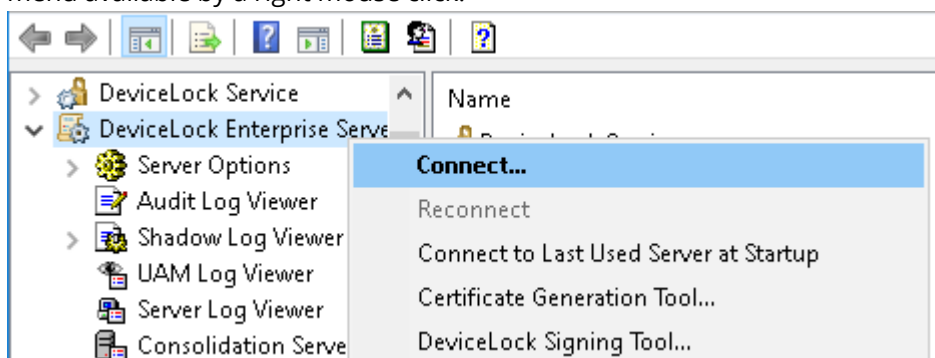
3. Double-click the **DeviceLock certificate** parameter to open the configuration dialog box.



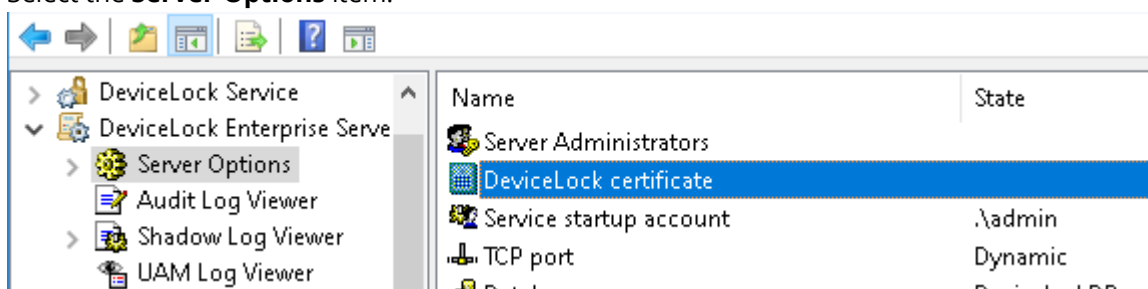
- Specify the path to the public key in the **Certificate Name** parameter if you want to install the certificate. You can use the **...** button to select the file with a public key.  
To remove the public key, use the **Remove** button.
- Click **OK** to close the configuration dialog box and apply changes.

To install/remove the private key on/from DeviceLock Enterprise Server and DeviceLock Content Security Server, you should use the DeviceLock Management Console as follows:

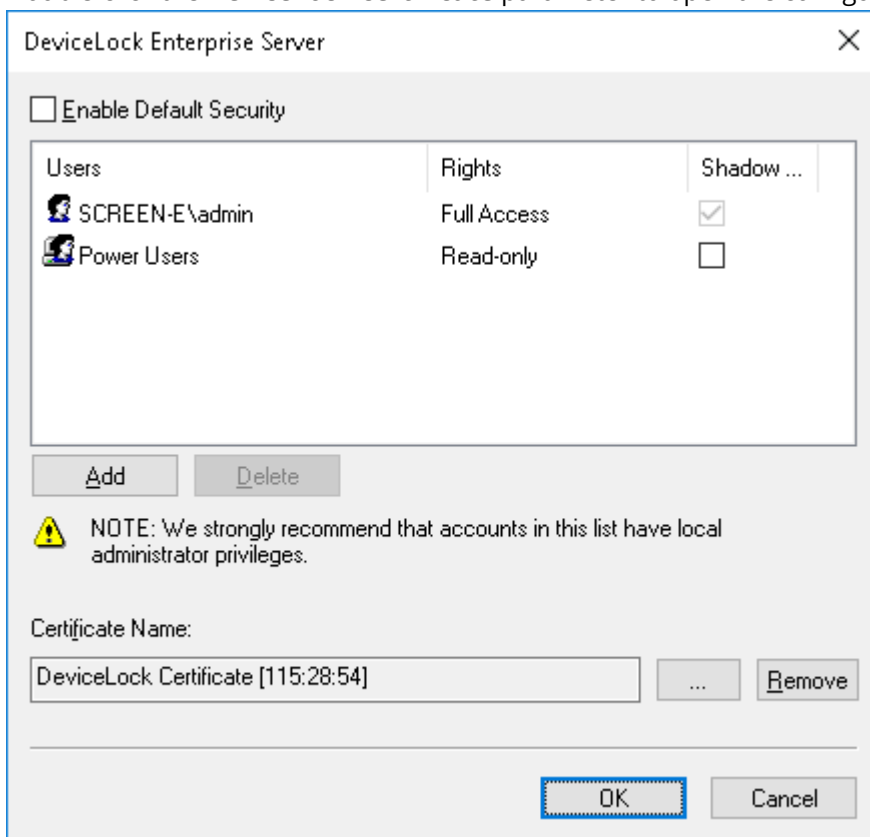
- Connect DeviceLock Management Console to the computer running DeviceLock Enterprise Server or DeviceLock Content Security Server. Use the **Connect** command from the shortcut menu available by a right mouse click.



- Select the **Server Options** item.



3. Double-click the **DeviceLock certificate** parameter to open the configuration dialog box.



4. Specify the path to the private key in the **Certificate Name** parameter if you want to install the certificate. Use the **...** button to select the file with a private key. To remove the private key, use the **Remove** button.
5. Click **OK** to close the configuration dialog box and apply changes.

For more information about installing the private key on DeviceLock Enterprise Server and DeviceLock Content Security Server, refer to the [Installing DeviceLock Enterprise Server](#) section (see the [Certificate Name](#) parameter description for DeviceLock Enterprise Server) and [Installing DeviceLock Content Security Server](#) section (see the [Certificate Name](#) parameter description for DeviceLock Content Security Server).

## DeviceLock Signing Tool

The DeviceLock Signing Tool is used to grant users temporary access to requested devices and sign files containing DeviceLock Service settings exported from DeviceLock Management Console or DeviceLock Group Policy Manager.

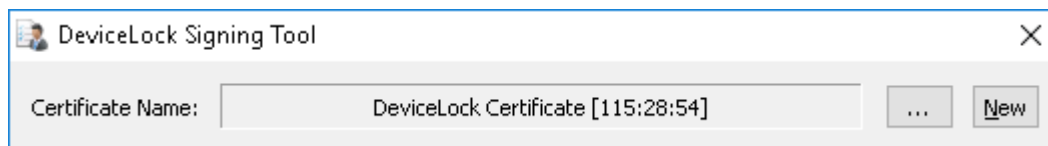
To run the DeviceLock Signing Tool, select **DeviceLock Signing Tool** from the **File** menu in DeviceLock Enterprise Manager or from the shortcut menu in DeviceLock Management Console or DeviceLock Service Settings Editor.

First of all you should load the private key of the DeviceLock Certificate.



The DeviceLock Signing Tool must use the private key that belongs to the same certificate as the public key installed on the user's computer.

By default, the DeviceLock Signing Tool automatically loads the last certificate used. You can load another certificate by pressing the **...** button and selecting a file with the private key.

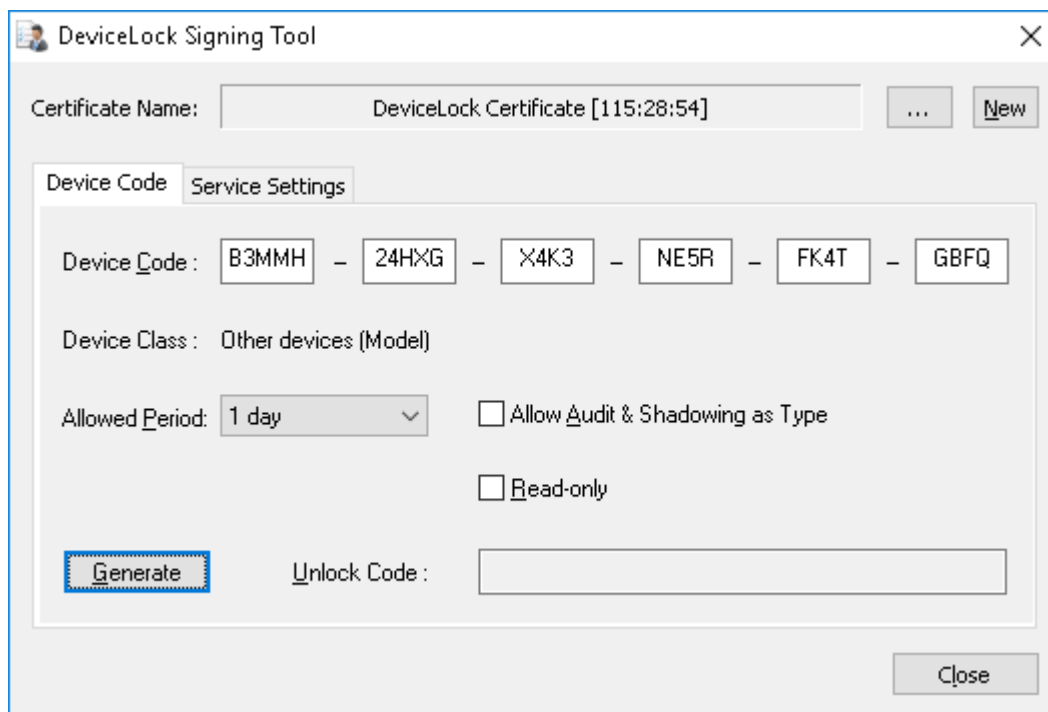


To generate a new certificate you can run the Certificate Generation Tool (see [Generating DeviceLock Certificates](#)) directly from the DeviceLock Signing Tool. To do so, you should click the **New** button. However, please keep in mind that if you generate a new certificate and intend to use its new private key in the DeviceLock Signing Tool, you must also deploy the corresponding public key on the user's computer.

Then, decide what action you want to perform: generate an unlock code (see [Device Code](#)) or sign a file containing DeviceLock Service settings (see [Service Settings](#)).

## Device Code

To grant the user temporary access to a requested device you should generate an Unlock Code upon receiving the Device Code from that user. For more information, refer to the [Temporary White List](#) section.



There are four simple steps to generating an Unlock Code for the user:

1. Load the DeviceLock Certificate private key as described [earlier](#).
2. Enter the Device Code, the user provides to you.

As soon as the correct Device Code is entered, you can see the class of the device the user wants access to in the **Device Class** field. The device class information helps you to control what kind of device the user is going to use. If, for example, a user declares the use of a USB scanner while actually trying to access a USB flash drive, the administrator would recognize the discrepancy. There is also a field (in round brackets) showing whether the requested device can be authorized as a unique device (**Unique**) or can be authorized only as a model (**Model**), i.e. whether or not it has a serial number. If you authorize the device as a model, then the user is granted access to all devices of this model. For more information on this, refer to the [USB Devices White List \(Regular Profile\)](#) section of this manual.
3. Select the period when the requested device will be allowed. In **Allowed Period**, you can select several predefined periods: 5, 15, 30, 60 minutes, 5 hours, 1 or 2 days, 1 or 2 weeks, 1 month, until the device is unplugged or until the user is logged off.

When you select a fixed time period (e.g. 10 minutes), the user is granted access to the requested device for only this period. As soon as the allowed time expires, access to the device is denied again. It doesn't matter what the user is doing with this device - even if copying files onto the USB disk or printing a document on the USB printer is in progress, all operations will be aborted.

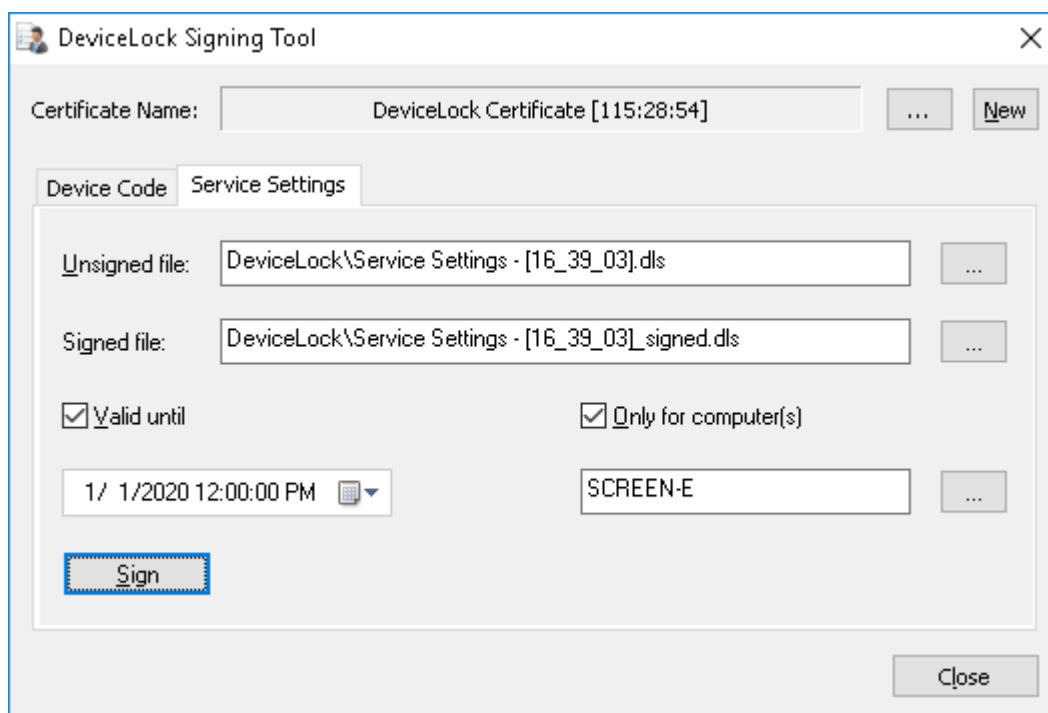
To allow the user to use a requested device without any time limitations, select **until unplug** in **Allowed Period**. The user is then granted access to the device while it is plugged into the port. As soon as the user unplugs this device, access to it is denied again.
4. Click the **Generate** button to create an Unlock Code. Provide this code to the user over the phone or in any other suitable way.

*The process of generating an Unlock Code depends upon your computer's processing speed and could take up to several seconds.*

## Service Settings

To avoid unauthorized modification you can sign a file containing DeviceLock Service settings exported from DeviceLock Management Console or DeviceLock Group Policy Manager or created using DeviceLock Service Settings Editor.

Later this file can be sent to users whose computers are not online and thus out-of-reach via management consoles.



There are six simple steps to signing a settings file:

1. Load the DeviceLock Certificate private key as described [earlier](#).
2. Load the file with DeviceLock Service settings to sign.  
The full path to this file must be specified in the **Unsigned file** field. You can use the **...** button to select the file.

*The file with DeviceLock Service settings can be created using the Save Service Settings command from the shortcut menu in DeviceLock Management Console, DeviceLock Group Policy Manager or DeviceLock Service Settings Editor.*

3. In the **Signed file** field, specify the resultant file. You can use the **...** button to select the folder where this file will be created.
4. Decide whether the resultant file should contain expiration information or not.  
If you want to allow users to import settings from this file without any time limitations, clear the **Valid until** check box.

If you select the **Valid until** check box and specify the date/time, then the expiration information is written to the resultant file and users can import settings from this file only before the specified date/time.

Please note that this parameter affects only users that are trying to import DeviceLock Service settings via the DeviceLock applet from the Windows Control Panel. When a file with settings is loaded using **Load Service Settings** from the shortcut menu in the DeviceLock Management Console or DeviceLock Group Policy Manager, the expiration information (if any) is ignored.

5. Decide whether the resultant file can be used only on specific computers or not.  
If you want to allow users to import settings from this file on any computers, clear the **Only for computer(s)** check box.

If you select the **Only for computer(s)** check box and specify the computer name then users will be able to import settings from this file only on this specified computer. Using the semicolon (;) as a separator, you can specify several computer names such that the resultant file can be used on any of these computers.


---

**Note**

You can't use the computer's IP address in this parameter. You must specify the computer name exactly as it is displayed in the System applet from the Windows Control Panel.

On Mac computers the name reported by the **hostname** command must be used. The same name is available in **System Preferences > Sharing**.

---

You can also load a predefined list of computers from the external text file. To open an external file, click the  button. This text file must contain each computer's name on separate lines.

Please note that this parameter affects only users that are trying to import DeviceLock Service settings via the **DeviceLock** applet from the Windows Control Panel. When a file with settings is loaded using **Load Service Settings** from the shortcut menu in the DeviceLock Management Console or DeviceLock Group Policy Manager, the computer's name information is ignored.

6. Click the **Sign** button to create a signed file with DeviceLock Service settings. Provide this file to the user in any suitable way.

*The process of file signing can be a time-consuming operation. It depends on your computer's processing speed and could take as long as several seconds.*

## Command-line options to sign a settings file

Another way to sign a settings file is by running `DLTempAccessAdmin.exe` from a command prompt. The file `DLTempAccessAdmin.exe` is located in the DeviceLock installation folder:

- `%ProgramFiles%\DeviceLock\` on a 32-bit system by default.
- `%ProgramFiles(x86)%\DeviceLock\` on a 64-bit system by default.

At a command prompt, switch to the DeviceLock installation folder, and use the following syntax to sign a settings file:

```
DLTempAccessAdmin.exe -s <in-file> -d <out-file> [-c <key-file>]
```

Option values in this syntax:

- `<in-file>` - The path and name of the settings file to sign.
- `<out-file>` - The path and name of the output signed settings file.
- `<key-file>` - The path and name of the file containing the private key of the DeviceLock certificate.

Example:

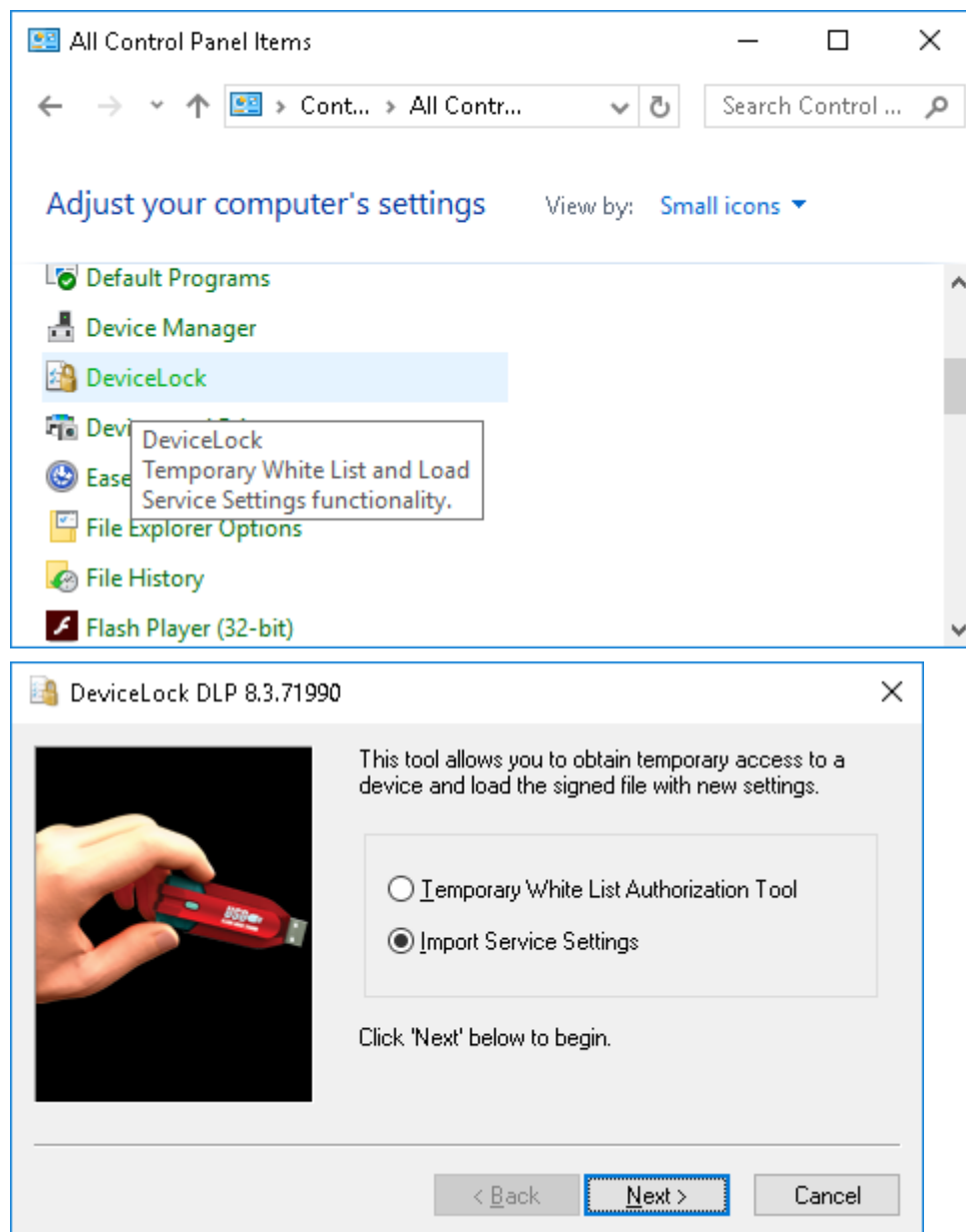
```
DLTempAccessAdmin.exe -s c:\temp\src.dls -d c:\temp\signed.dls -c c:\temp\private
```

Option `-c <key-file>` is not required. If this option is omitted, the file is signed using the key that was last used in the Signing Tool. Otherwise, the Signing Tool remembers the key specified by this option, and uses it in future operations by default.

If the file path or name contains spaces, the option value must be enclosed in quotation marks, such as `-s "c:\temp\my settings"`.

## Loading signed settings file on Windows

To apply DeviceLock Service settings from a signed file, the user should run the **DeviceLock** applet in Control Panel and select the **Import Service Settings** option.




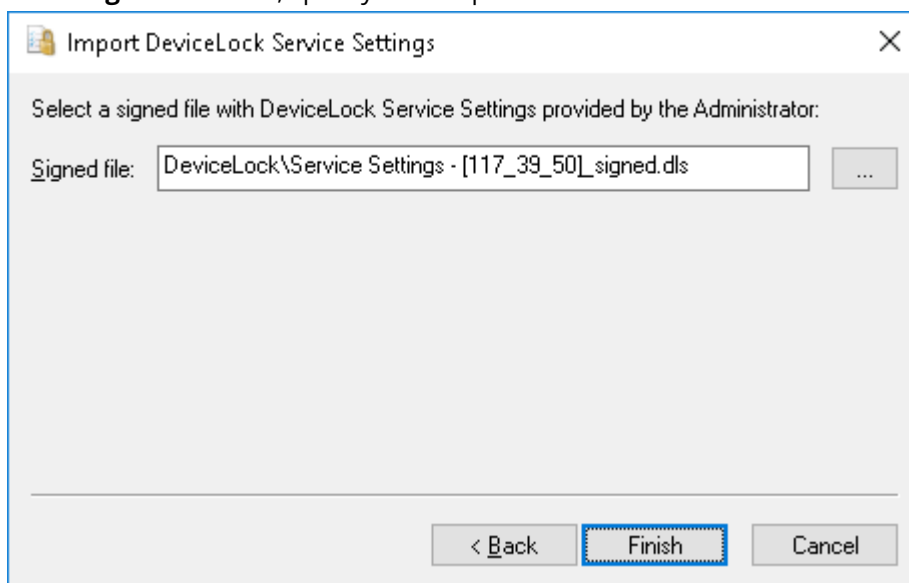
---

**Note**

- To access the DeviceLock applet, the user has to switch Control Panel to the “Small icons” view mode.
  - The caption of the applet window displays the DeviceLock version and build number.
  - The DeviceLock applet may fail to start, returning the “Certificate is not installed” error. To resolve this issue, install the public key of the DeviceLock certificate on the client computer. For installation instructions, see [Installing/Removing DeviceLock Certificate](#).
- 

To load the settings from a signed file, the user has to perform two simple steps:

1. In the **Signed file** field, specify the full path to the file. Click the  button to select the file.



2. Click the **Finish** button.

If the digital signature in the file is valid, then the new settings will be applied to DeviceLock Service immediately. The following message will appear: “File has been successfully loaded.”

The user can also use the command line to load the signed file with DeviceLock Service settings:

```
DLTempAccess.cpl -s <path to signed file>
```

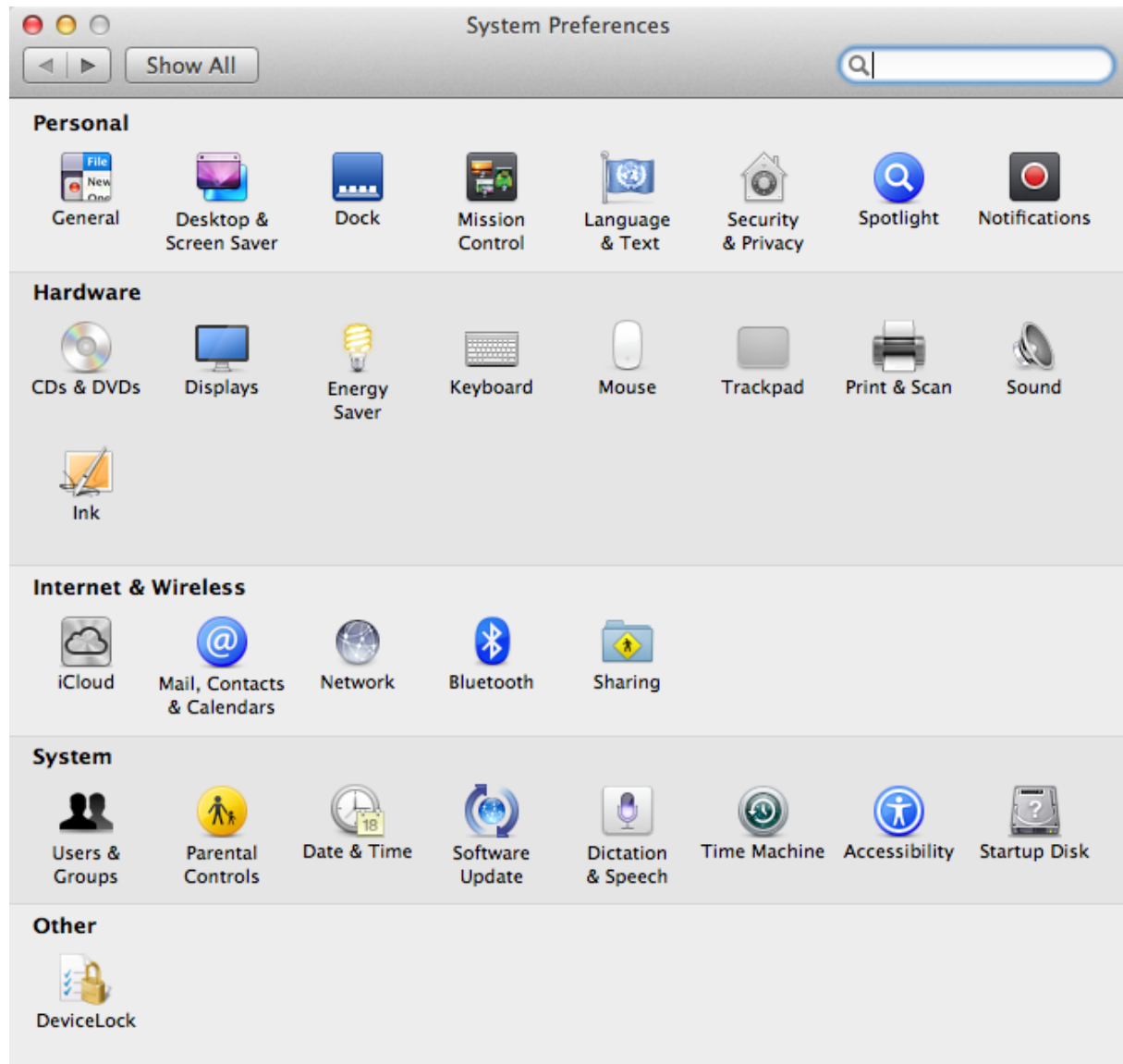
In this syntax <path to signed file> is the path to the signed file with DeviceLock Service settings. For example:

```
DLTempAccess.cpl -s "C:\Program Files\DeviceLock\settings_signed.dls"
```

All successful attempts to load settings are logged, if logging of changes is enabled in [Service Options](#) (see the [Log Policy changes and Start/Stop events](#) parameter description).

## Loading signed settings file on Mac

DeviceLock Service for Mac installs its Preference Pane into System Preferences at **System Preferences > DeviceLock**.



To load the settings from a signed file, the user should run the **DeviceLock** pane from System Preferences, click **Next** in the dialog box that appears, and then perform the following steps:

1. Specify the full path to the signed settings file. Use the **Browse** button to select the file.
2. Click the **Apply** button.

If the digital signature in the file is valid, then the new settings will be applied to DeviceLock Service for Mac immediately. The following message will appear: "File has been successfully loaded."

The user can also load the signed file with DeviceLock Service settings using the command line:

```
/Library/DeviceLockAgent/Utilities/DLAgentControl importdls <path to signed file>
```

In this syntax <path to signed file> is the full path to the signed file with DeviceLock Service settings. For example:

```
/Library/DeviceLockAgent/Utilities/DLAgentControl importdls /home/user/Desktop/settings_  
signed.dls
```

---

**Note**

If DeviceLock Administrators are configured, a non-administrative user will not be able to access the /Library/DeviceLockAgent/Utilities folder even in read-only mode. The administrator must copy DLAgentControl to a different location. Alternatively, the application is available in the Utilities folder on the installation .dmg image.

---

All successful attempts to load settings are logged, if logging of changes is enabled in [Service Options](#) (see the [Log Policy changes and Start/Stop events](#) parameter description).



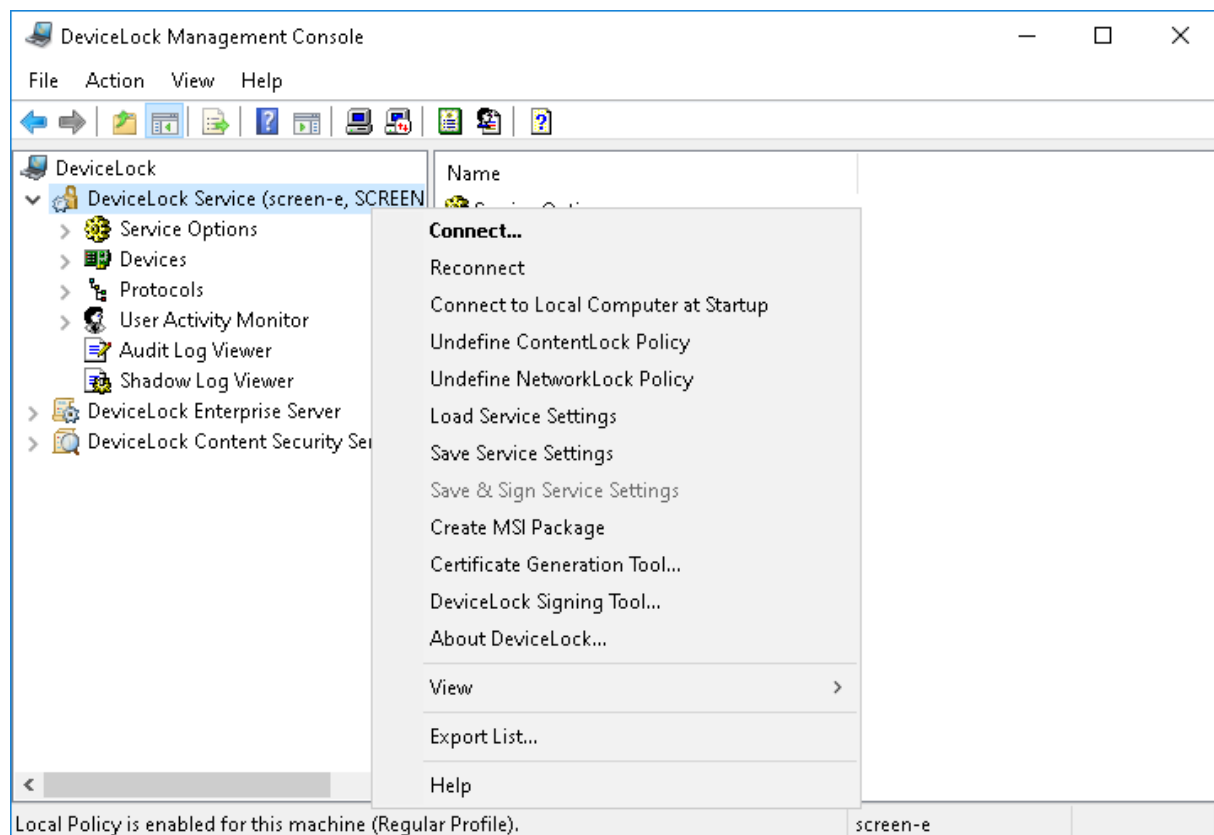
# DeviceLock Service

## Managing DeviceLock Service for Windows

Expand the **DeviceLock Service** node in the console tree to access all the service function and configuration settings.

### Important

To view or change service settings in the DeviceLock Management Console, you must first connect it to the computer running the DeviceLock Service. See [Connecting to Computers](#) for details.



The shortcut menu of the **DeviceLock Service** node provides the following commands:

- **Connect** - Connects to the computer you specify. See [Connecting to Computers](#) for details.
- **Reconnect** - Connects to the currently connected computer once again.
- **Connect to Local Computer at Startup** - Click to select or clear the check box next to this command. When selected, it forces the DeviceLock Management Console to connect to the local computer automatically each time the console starts.
- **Undefine ContentLock Policy** - Resets all parameters specific to ContentLock (all Content-Aware Rules except those based on file types) to the unconfigured state.
- **Undefine NetworkLock Policy** - Resets all parameters specific to NetworkLock to the unconfigured state.

- **Load Service Settings** - Loads settings from a DeviceLock Service settings file. You need to select a file created by saving DeviceLock Service settings in DeviceLock Service Settings Editor, DeviceLock Management Console, or DeviceLock Group Policy Manager. This could be a signed or non-signed file.
- **Save Service Settings** - Saves the DeviceLock Service current settings to a settings file. Later this file can be loaded to DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor. This file can also be sent to users whose computers are not on-line and thus out-of-reach via management consoles. To avoid tampering with the settings file, it should be signed using [DeviceLock Signing Tool](#). See also [Settings file save options](#).
- **Save & Sign Service Settings** - Saves the DeviceLock Service current settings to a settings file and signs it the private key of the last-used DeviceLock certificate. This command is unavailable if DeviceLock Signing Tool has never used a DeviceLock certificate's private key. See also [Settings file save options](#).
- **Create MSI Package** - Creates a custom MSI package for installing DeviceLock Service with the settings identical to the DeviceLock Service current settings.  
When using this command, you first need to select a source MSI package for DeviceLock Service. This may be one of MSI packages that ship with DeviceLock (such as DeviceLock Service.msi and DeviceLock Service x64.msi).  
Then you need to specify the name of the resultant (target) MSI package that will be generated based on the source MSI package and the DeviceLock Service current settings.  
Later this custom MSI package can be used to deploy DeviceLock Service across the network with predefined policies (see [Installation via Group Policy](#)).

---

#### Note

When a custom MSI package is used to deploy DeviceLock Service via Group Policy, these service settings held in that package are not applied to client computers if any one of the following conditions is true:

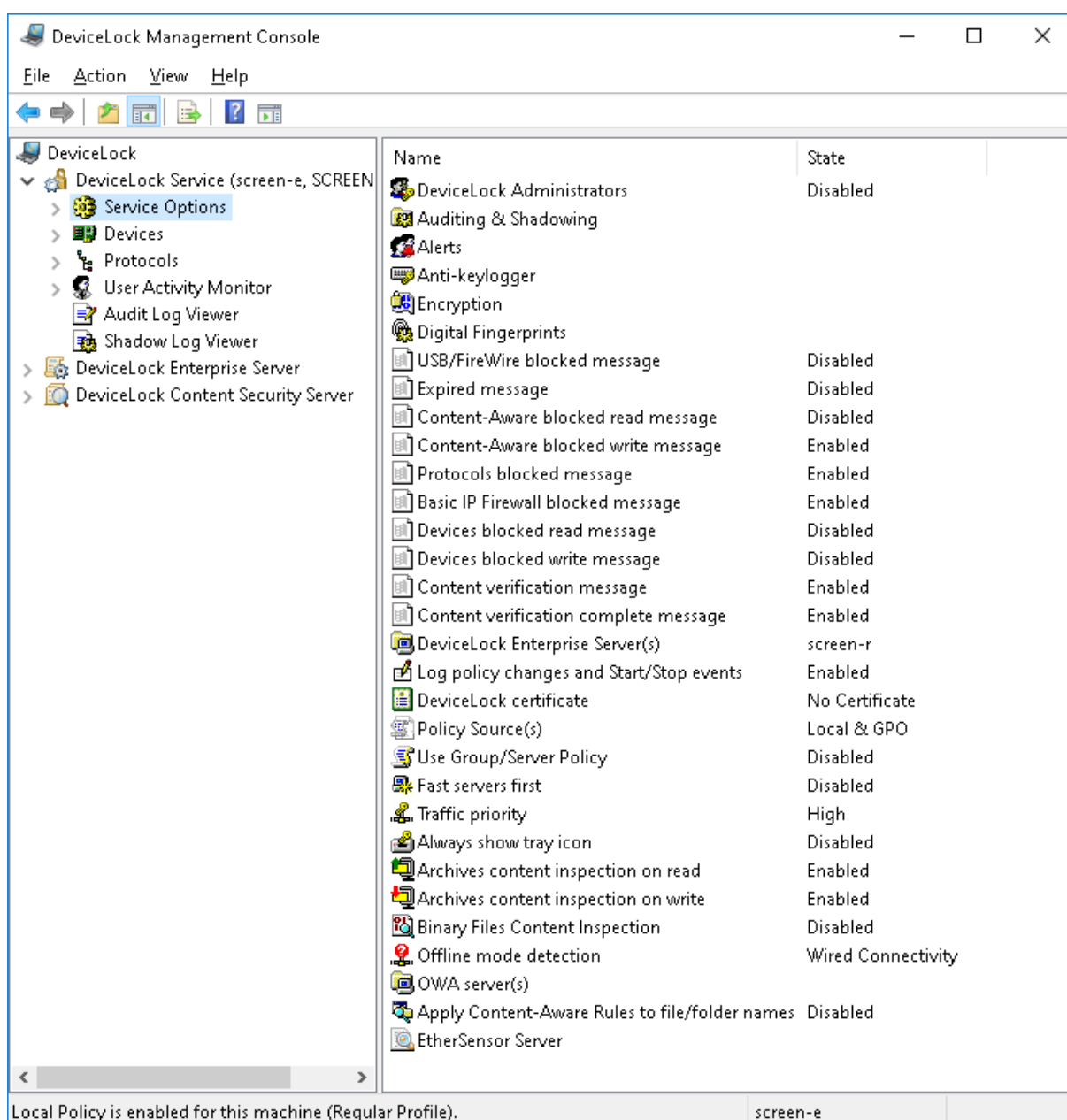
- The default security is disabled on remotely running DeviceLock Services.
  - The GPO applied to client computers has the **Override Local Policy** setting enabled.
- 

Please note that the **Create MSI Package** menu item is disabled when there is no Microsoft Windows Installer (version 1.0 or later) installed on the local computer.

- **Certificate Generation Tool** - Starts a tool for generating DeviceLock Certificates. See [Generating DeviceLock Certificates](#) for details.
- **DeviceLock Signing Tool** - Starts a tool for granting users temporary access to requested devices and sign DeviceLock Service settings files. See [DeviceLock Signing Tool](#) for details.
- **About DeviceLock** - Displays a dialog box with information about the DeviceLock version and licenses.

## Service Options

These additional parameters allow you to tune up the DeviceLock Service configuration. Use the shortcut menu available by a right mouse click on every parameter.



When configuring DeviceLock Service options, consider the following:

- The DeviceLock Service options may unexpectedly revert to default settings and the DeviceLock Management Console displays a warning message: "This machine is configured to use Group Policy settings." This message indicates that the DeviceLock Service works in Group Policy mode. The local settings are overridden by the ones from a Group Policy Object.
- To use local settings for DeviceLock Service, disable the [Use Group/Server Policy](#) option. Otherwise, configure DeviceLock Service options in the Group Policy Object that affects the client computer (for instructions, see [DeviceLock Group Policy Manager](#)). One more way to configure DeviceLock Service options is by using [DeviceLock Enterprise Server Policies](#).
- DeviceLock Service can receive its settings from the Acronis cyber protection system. The status bar of the DeviceLock Management Console displays the message "Acronis Cyber Protect Policy is enabled for this machine" and you cannot change the settings by using the DeviceLock

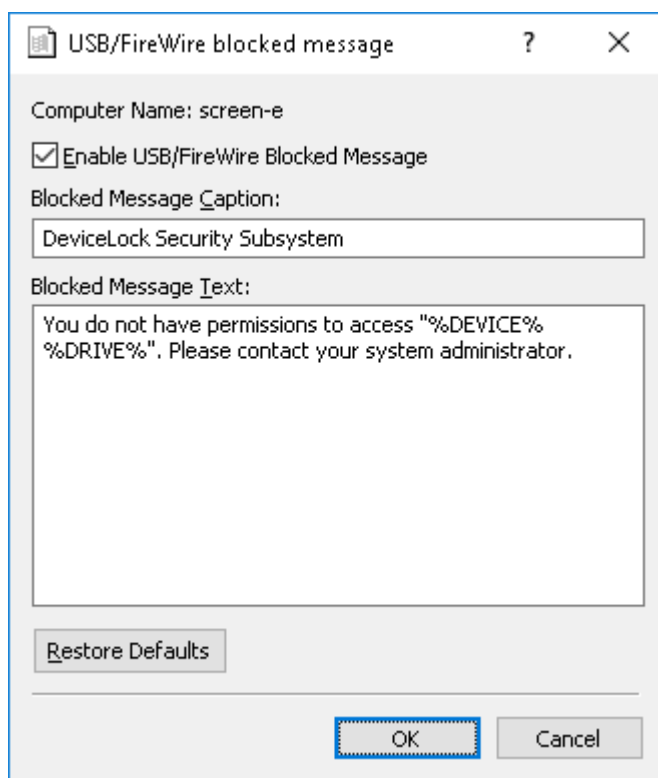
Management Console. To manage DeviceLock Service in this case, you need to use the Acronis cyber protection service console.

The service options are as follows:

- [USB/FireWire blocked message](#)
- [Expired message](#)
- [Content-Aware blocked read message](#)
- [Content-Aware blocked write message](#)
- [Protocols blocked message](#)
- [Basic IP Firewall blocked message](#)
- [Devices blocked read message](#)
- [Devices blocked write message](#)
- [Content verification message](#)
- [Content verification complete message](#)
- [DeviceLock Enterprise Server\(s\)](#)
- [Log Policy changes and Start/Stop events](#)
- [DeviceLock certificate](#)
- [Policy Source\(s\)](#)
- [Use Group/Server Policy](#)
- [Fast servers first](#)
- [Traffic priority](#)
- [Always show tray icon](#)
- [Archives content inspection on read](#)
- [Archives content inspection on write](#)
- [Binary Files Content Inspection](#)
- [Offline mode detection](#)
- [OWA server\(s\)](#)
- [Apply Content-Aware Rules to file/folder names](#)
- [EtherSensor Server](#)
- [DeviceLock Administrators](#)
- [Auditing & Shadowing](#)
- [Alerts](#)
- [Anti-keylogger](#)
- [Encryption](#)
- [Digital Fingerprints](#)

## USB/FireWire blocked message

You can define a custom message to be displayed to users when a USB or FireWire device that is denied at the interface (USB or FireWire) level or type (Removable, Optical Drive, etc.) level is plugged in.



To enable this custom message, select the **Enable USB/FireWire Blocked Message** check box.

Also, you can define additional parameters, such as:

- **Blocked Message Caption** - The text to be displayed as a caption.
- **Blocked Message Text** - The main text of the message.

The following macros can be added to the message caption and/or message text to make the message more meaningful to the user:

- %TYPE% - Inserts the port name (USB port, FireWire port) where the device is plugged.
- %DEVICE% - Inserts the name of the device (e.g. USB Mass Storage Device) received from the system.
- %DRIVE% - Inserts the drive letter of the storage device (e.g. F:). If the device doesn't have a letter, then this macro inserts an empty string.

---

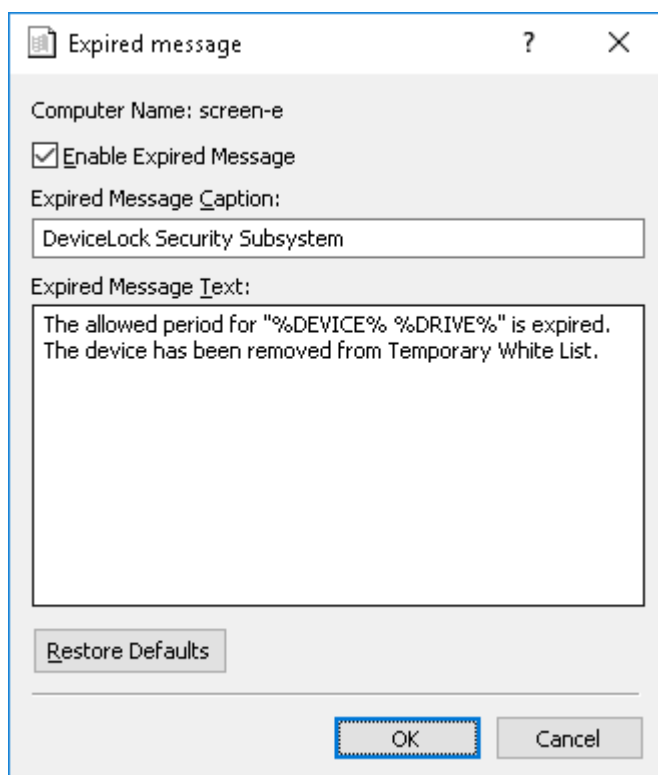
#### Note

In case of a terminal server session, the message may be displayed to all logged-on users who don't have permission to use USB or FireWire ports when any one of them attempts to use that port.

---

## Expired message

You can define a custom message to be displayed to users when the allowed period for temporary white listed devices is expired and devices have been removed from [Temporary White List](#).



To enable this custom message, select the **Enable Expired Message** check box.

Also, you can define additional parameters, such as:

- **Expired Message Caption** - The text to be displayed as a caption.
- **Expired Message Text** - The main text of the message.

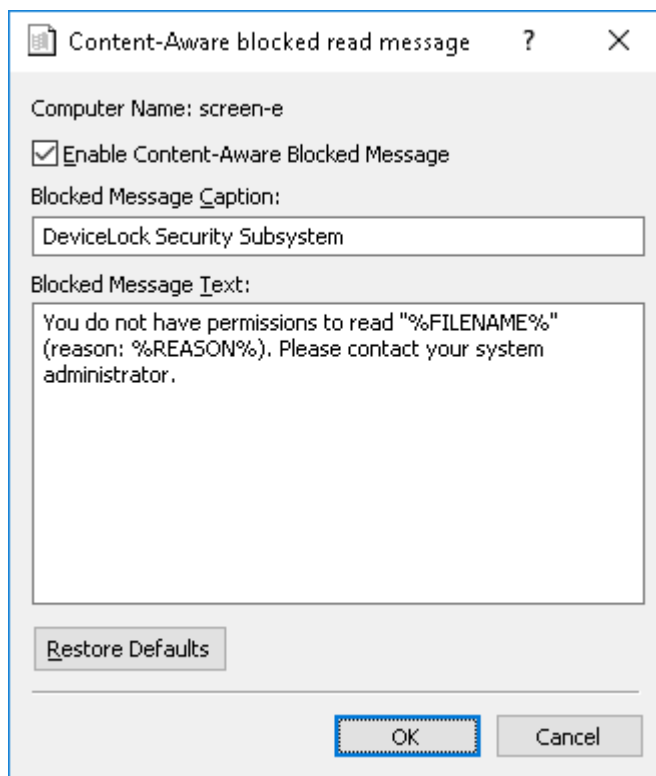
The following macros can be added to the message caption and/or message text to make the message more meaningful to the user:

- **%DEVICE%** - Inserts the name of the device (e.g. USB Mass Storage Device) received from the system.
- **%DRIVE%** - Inserts the drive letter of the storage device (e.g. F:). If the device doesn't have a letter, then this macro inserts an empty string.

## Content-Aware blocked read message

You can define a Content-Aware blocked read message (notification balloon) to be displayed to users when they try to read a file to which they are denied access. This message balloon is shown in the notification area of the taskbar on client computers. By default, DeviceLock does not display the Content-Aware blocked read message.

To enable or disable the Content-Aware blocked read message, right-click **Content-Aware blocked read message** and then click **Properties**, or double-click **Content-Aware blocked read message**.



In the **Content-Aware blocked read message** dialog box, do the following:

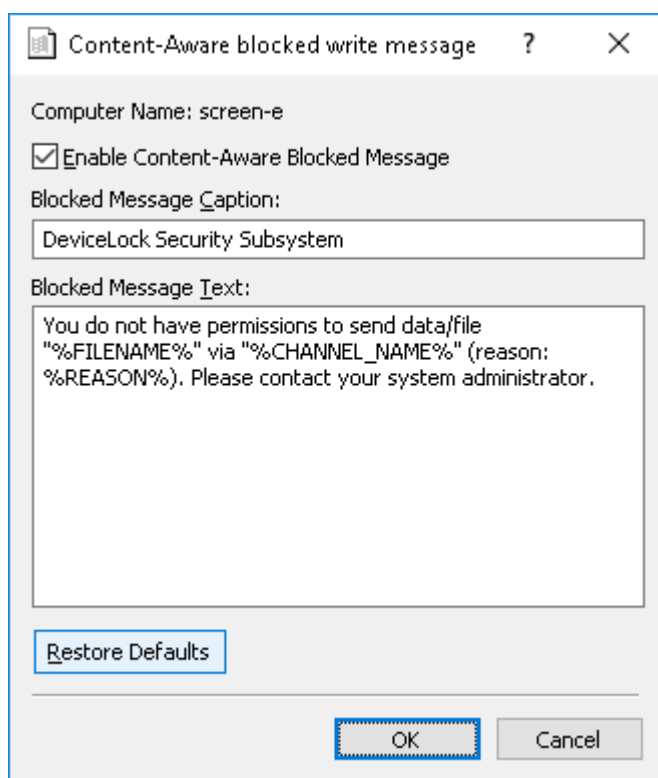
- **Enable Content-Aware Blocked Message** - Enable or disable the display of the Content-Aware blocked read message.  
Select the **Enable Content-Aware Blocked Message** check box to enable the display of the message.  
Clear the **Enable Content-Aware Blocked Message** check box to disable the display of the message.
- **Blocked Message Caption** - Specify the text to display in the title bar of the message balloon.  
The default message caption is as follows: "DeviceLock Security Subsystem"
- **Blocked Message Text** - Specify the text to display in the message balloon.  
The default message text is as follows: "You do not have permissions to read \"%FILENAME%\" (reason: %REASON%). Please contact your system administrator."  
In this message, %FILENAME% provides the path and file name, %REASON% describes why access to the file is denied.
- **Restore Defaults** - Restore the default settings.

For details on the Content-Aware Rules feature, see [Content-Aware Rules \(Regular Profile\)](#).

## Content-Aware blocked write message

You can define a Content-Aware blocked write message (notification balloon) to be displayed to users when they try to write a file or transfer the data to which they are denied access. This message balloon is shown in the notification area of the taskbar on client computers. By default, DeviceLock displays the Content-Aware blocked write message.

To enable or disable the Content-Aware blocked write message, right-click **Content-Aware blocked write message** and then click **Properties**, or double-click **Content-Aware blocked write message**.



In the **Content-Aware blocked write message** dialog box, do the following:

- **Enable Content-Aware Blocked Message** - Enable or disable the display of the Content-Aware blocked write message.  
Select the **Enable Content-Aware Blocked Message** check box to enable the display of the message.  
Clear the **Enable Content-Aware Blocked Message** check box to disable the display of the message.
- **Blocked Message Caption** - Specify the text to display in the title bar of the message balloon.  
The default message caption is as follows: "DeviceLock Security Subsystem"
- **Blocked Message Text** - Specify the text to display in the message balloon.  
The default message text is as follows: "You do not have permissions to send data/file \"%FILENAME%\" via \"%CHANNEL\_NAME%\" (reason: %REASON%). Please contact your system administrator."  
In this message, %FILENAME% provides the path and file name, %CHANNEL\_NAME% identifies the data transmission channel, %REASON% describes why access to the file is denied.
- **Restore Defaults** - Restore the default settings.

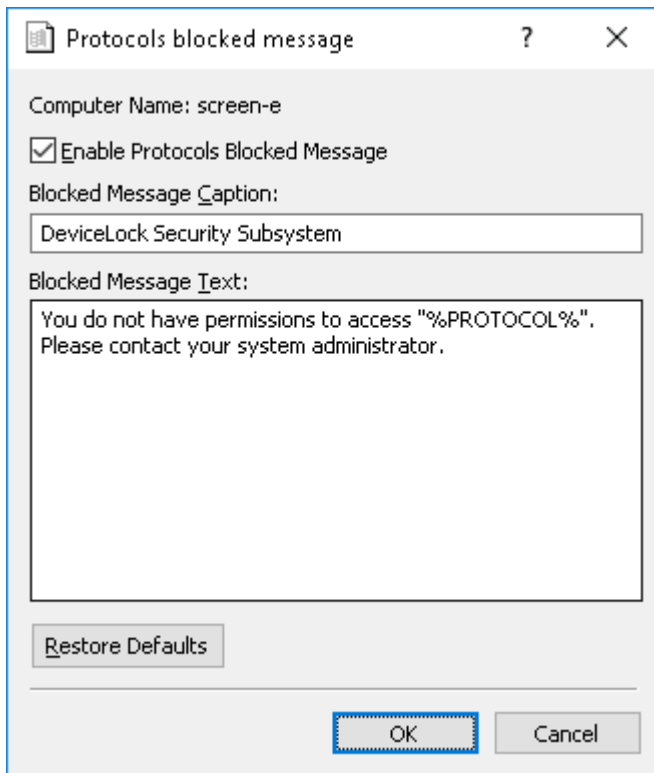
For details on the Content-Aware Rules feature, see [Content-Aware Rules \(Regular Profile\)](#).



## Protocols blocked message

You can define a Protocols blocked message (notification balloon) to be displayed to users when they try to access a protocol to which they are denied access. This message balloon is shown in the notification area of the taskbar on client computers.

To enable or disable the Protocols blocked message, right-click **Protocols blocked message**, and then click **Properties**, or double-click **Protocols blocked message**.



In the **Protocols blocked message** dialog box, do the following:

- **Enable Protocols Blocked Message** - Enable or disable the display of the Protocols blocked message.  
Select the **Enable Protocols Blocked Message** check box to enable the display of the message.  
Clear the **Enable Protocols Blocked Message** check box to disable the display of the message.
- **Blocked Message Caption** - Specify the text to display in the title bar of the message balloon.  
The default message caption is as follows: "DeviceLock Security Subsystem"
- **Blocked Message Text** - Specify the text to display in the message balloon.  
The default message text is as follows: "You do not have permissions to access \"%PROTOCOL%\". Please contact your system administrator."
- **Restore Defaults** - Restore the default settings.

The following macros can be added to the message caption and/or message text to make the message more meaningful to the user:

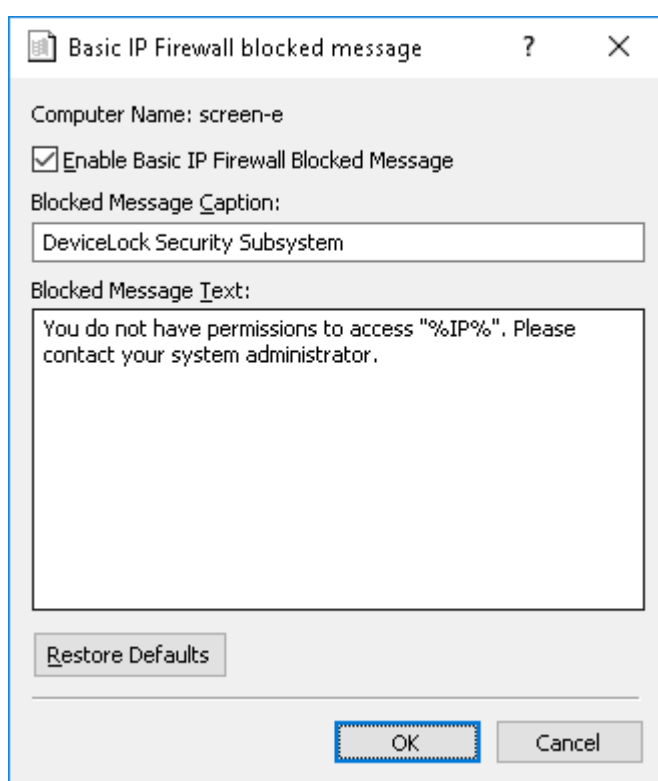
- %PROTOCOL% - Inserts the name of the protocol that is blocked.
- %IP% - Inserts the IP address and/or the name of the resource of which access is blocked. If the resource name cannot be identified, only the IP address is displayed. If the IP address cannot be identified, only the resource name is displayed.

For a details on the Protocols feature, see [Protocols \(Regular Profile\)](#).

## Basic IP Firewall blocked message

You can define a Basic IP Firewall blocked message to be displayed to users when they try to establish a connection to which they are denied access.

To enable or disable the Basic IP Firewall blocked message, right-click **Basic IP Firewall blocked message**, and then click **Properties**, or double-click **Basic IP Firewall blocked message**.



In the **Basic IP Firewall blocked message** dialog box, do the following:

- **Enable Basic IP Firewall Blocked Message** - Enable or disable the display of the Basic IP Firewall blocked message.  
Select the **Enable Basic IP Firewall Blocked Message** check box to enable the display of the message.  
Clear the **Enable Basic IP Firewall Blocked Message** check box to disable the display of the message.
- **Blocked Message Caption** - Specify the text to display in the title bar of the message box.  
The default message caption is as follows: "DeviceLock Security Subsystem"

- **Blocked Message Text** - Specify the text to display in the message box.

The default message text is as follows: "You do not have permissions to access "%IP%". Please contact your system administrator."

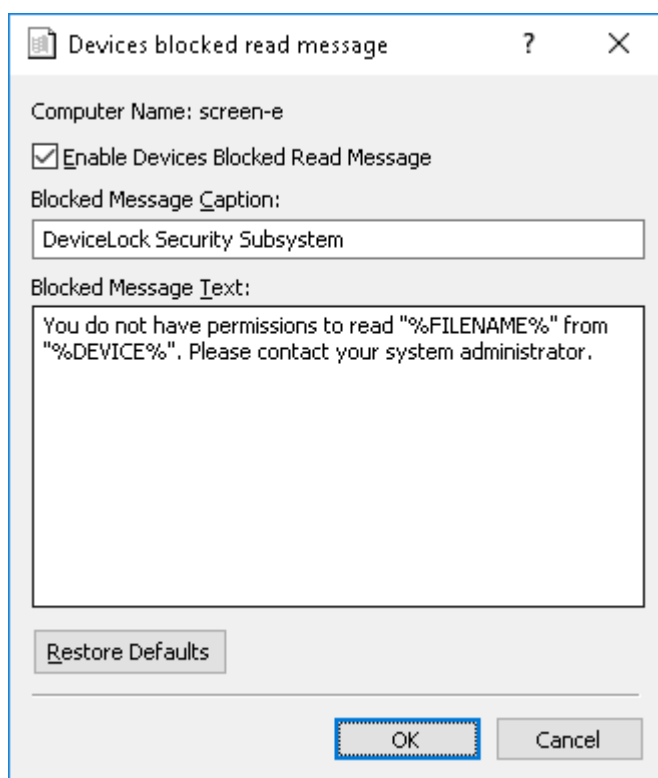
In place of %IP% the message displays the IP address and/or the name of the host of which access is blocked. If the host name cannot be identified, the message only displays the IP address. If the IP address cannot be identified, then only the host name is displayed.

- **Restore Defaults** - Restore the default settings.

For details on the Basic IP Firewall feature, see [Managing Basic IP Firewall](#).

## Devices blocked read message

This option defines a message to display to users when denying read access to the following device types: Floppy, Hard disk, Optical Drive, Removable, Tape, MTP, iPhone, Palm, Windows Mobile, TS Devices (upon denying Mapped Drives Read, Clipboard Incoming Text, Clipboard Incoming Image, Clipboard Incoming Audio, Clipboard Incoming File, or Clipboard Incoming Unidentified Content).



To enable this custom message, select the **Enable Devices Blocked Read Message** check box.

---

**Note**

- The message is also displayed when denying read or write access to Blackberry, Bluetooth, FireWire port, Infrared port, Serial port, Parallel port, TS Devices (upon denying Serial Port Access or USB Devices Access), USB port, WiFi.
  - The message is displayed to the user whose access rights lack read access permissions at the very moment an attempt to gain read access is made.
  - When denying read or write access to WiFi or Bluetooth, the message is displayed only once. There will be no further messages until the WiFi or Bluetooth settings are changed.
- 

Also, you can define additional parameters, such as:

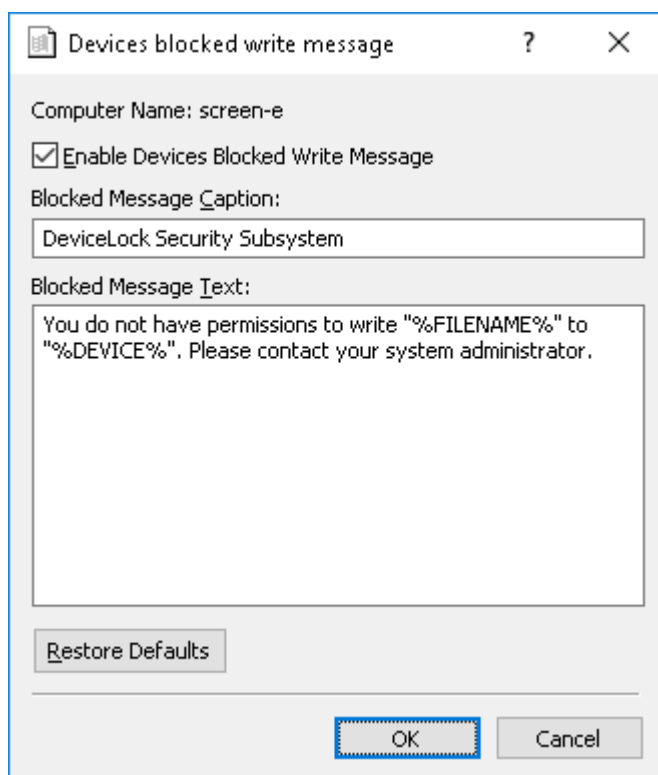
- **Blocked Message Caption** - The text to be displayed as a caption.
- **Blocked Message Text** - The main text of the message.

The following macros can be added to the message caption and/or message text to make the message more meaningful to the user:

- %FILENAME% - Inserts the name of the file to be read.
- %DEVICE% - Inserts the name of the device (e.g. USB Mass Storage Device) received from the system.

## Devices blocked write message

This option defines a message to display to users when denying write access to the following device types: Floppy, Hard disk, Optical Drive, Removable, Tape, MTP, iPhone, Palm, Windows Mobile, Printer, Clipboard (upon denying Copy Text, Copy File, Copy Image, Copy Audio, Copy Unidentified Content, or Screenshot), TS Devices (upon denying Mapped Drives Write, Clipboard Outgoing Text, Clipboard Outgoing Image, Clipboard Outgoing Audio, Clipboard Outgoing File, or Clipboard Outgoing Unidentified Content).



To enable this custom message, select the **Enable Devices Blocked Write Message** check box.

---

#### Note

- The message is displayed to the user whose access rights lack write access at the very moment an attempt to gain write access is made.
  - The message is not displayed when denying write access to Blackberry, Bluetooth, FireWire port, Infrared port, Serial port, Parallel port, TS Devices (upon denying Serial Port Access or USB Devices Access), USB port, WiFi. In this case, the devices blocked read message is displayed.
- 

Also, you can define additional parameters, such as:

- **Blocked Message Caption** - The text to be displayed as a caption.
- **Blocked Message Text** - The main text of the message.

The following macros can be added to the message caption and/or message text to make the message more meaningful to the user:

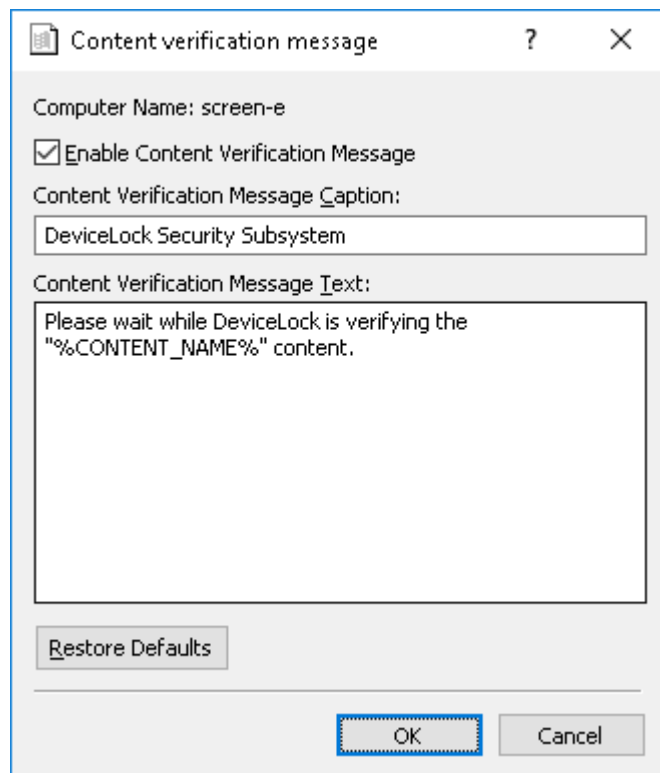
- **%FILENAME%** - Inserts the name of the file to be written.
- **%DEVICE%** - Inserts the name of the device (e.g. USB Mass Storage Device) received from the system.

## Content verification message

Checking the content of files copied to devices or transmitted over the network can be a time-consuming operation. You can define a Content verification message to be displayed to users when

content inspection is in progress. This message is displayed 20 seconds after DeviceLock Service starts checking the file content.

To enable or disable the Content verification message, right-click **Content verification message**, and then click **Properties**, or double-click **Content verification message**.



In the **Content verification message** dialog box, do the following:

- **Enable Content Verification Message** - Enable or disable the display of the Content verification message.  
Select the **Enable Content Verification Message** check box to enable the display of the message.  
Clear the **Enable Content Verification Message** check box to disable the display of the message.
- **Content Verification Message Caption** - Specify the text to display in the title bar of the message box.  
The default message caption is as follows: "DeviceLock Security Subsystem"
- **Content Verification Message Text** - Specify the text to display in the message box.  
The default message text is as follows: "Please wait while DeviceLock is verifying the \"%CONTENT\_NAME%\" content."  
In this message, %CONTENT\_NAME% is the name of the file or protocol to be inserted. The file name is inserted when DeviceLock checks the content of files copied to a device. The protocol name is inserted when DeviceLock checks the content of data transmitted over the network.
- **Restore Defaults** - Restore the default settings.

For details on the Content-Aware Rules feature, see [Content-Aware Rules \(Regular Profile\)](#).

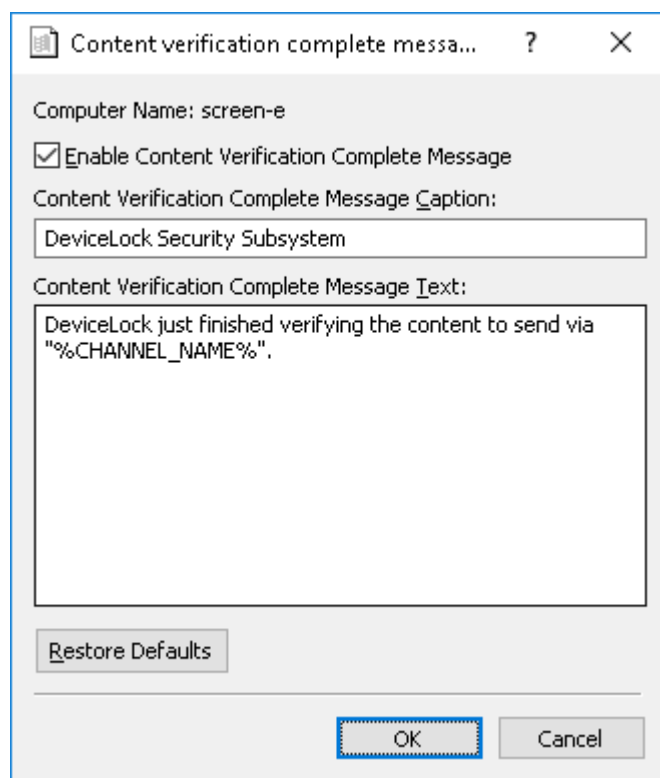
## Content verification complete message

You can define a Content verification complete message to be displayed to users when DeviceLock completes content inspection of data copied to Removable Devices or TS Devices (Mapped drives).

### Note

After this message is displayed, users can safely unplug the removable device using the Safely Remove Hardware utility. However, in some rare cases, we do not guarantee safe removal of the device immediately after this message is displayed.

To enable or disable the Content verification complete message, right-click **Content verification complete message**, and then click **Properties**, or double-click **Content verification complete message**.



In the **Content verification complete message** dialog box, do the following:

- **Enable Content Verification Complete Message** - Enable or disable the display of the Content verification complete message.  
Select the **Enable Content Verification Complete Message** check box to enable the display of the message.  
Clear the **Enable Content Verification Complete Message** check box to disable the display of the message.
- **Content Verification Complete Message Caption** - Specify the text to display in the title bar of the message box.  
The default message caption is as follows: "DeviceLock Security Subsystem"

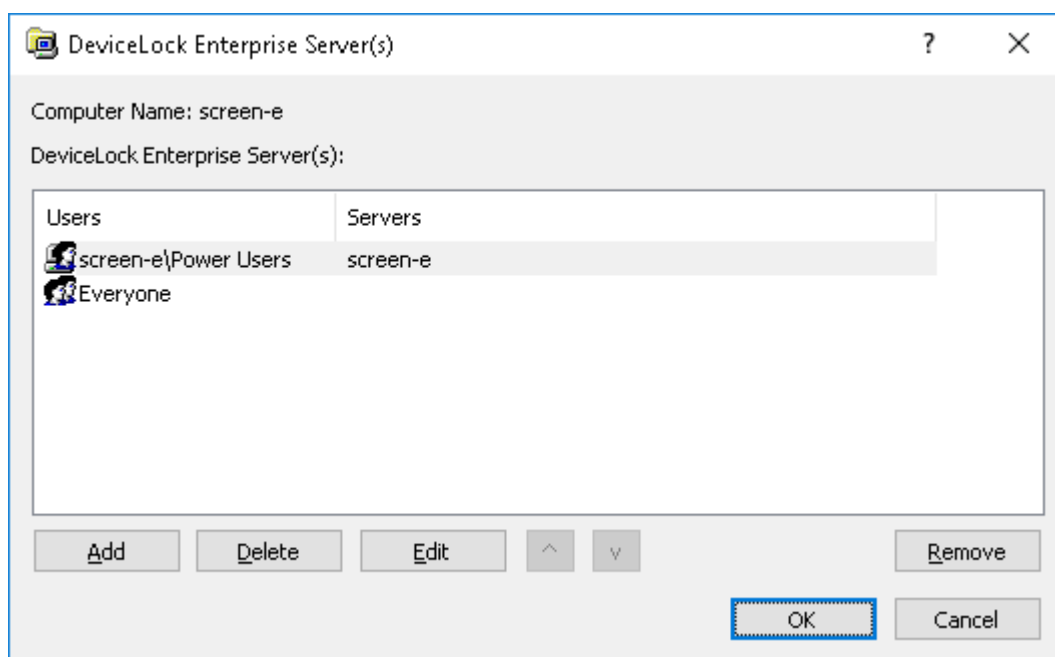
- **Content Verification Complete Message Text** - Specify the text to display in the message box. The default message text is as follows: "DeviceLock just finished verifying the content to send via "%CHANNEL\_NAME%"."
- In this message, %CHANNEL\_NAME% is the name of the data transmission channel to be inserted.
- **Restore Defaults** - Restore the default settings.

For details on the Content-Aware Rules feature, see [Content-Aware Rules \(Regular Profile\)](#).

## DeviceLock Enterprise Server(s)

If you want DeviceLock Service to send its log data to DeviceLock Enterprise Server, specify the name or IP address of the computer running that server. You can specify servers on a per-user or per-group basis. Log data that applies to the specified user or group is sent to the specified server. Another option is to specify a server for the Everyone group, which causes DeviceLock Service to send all log data to that server.

Double-click **DeviceLock Enterprise Server(s)** in the details pane to open the dialog box where you can configure the list of servers:



In the **DeviceLock Enterprise Server(s)** dialog box, you can view or change the list of servers:

- **Users** - Lists the users and user groups that have servers specified. Initially, the list contains only the Everyone group. Use the **Add** or **Delete** button to add or remove a user or group from the list. Clicking **Add** opens a regular dialog box for selecting users and groups. To remove all users and groups, except Everyone, click **Remove**. The Everyone group cannot be removed.
- **Servers** - For each user or group, specifies one or more computers running DeviceLock Enterprise Server. Click a user or group, and then click **Edit** to make changes to the **Servers** field for that user or group. Alternatively, press F2 or double-click in the **Servers** field.



DeviceLock Service sends the log data that applies to a given user or user group to the server specified in the **Servers** field for that user or group. If you specify a server for the Everyone group, DeviceLock Service sends any log data to that server.

It is possible to specify multiple servers by using a semicolon (;) to separate computer names in the **Servers** field. DeviceLock Service chooses one of these servers that is available on the network. The server choice also depends upon the [Fast servers first](#) setting in the **Service Options** list.

If a given user is assigned to multiple servers because of membership in multiple groups that are listed in the **DeviceLock Enterprise Server(s)** dialog box, then you can prioritize the servers by using the up and down arrow buttons to move those groups up or down in the list. DeviceLock Service will first attempt to use servers that are higher in the list. The servers that are only assigned to the Everyone group are always the last to choose: the Everyone group stands at the bottom of the list and it cannot be moved up.

Make sure that DeviceLock Enterprise Server is properly installed and accessible for DeviceLock Service; otherwise, logs will not be stored in the centralized database. For server installation steps, see [Installing DeviceLock Enterprise Server](#).

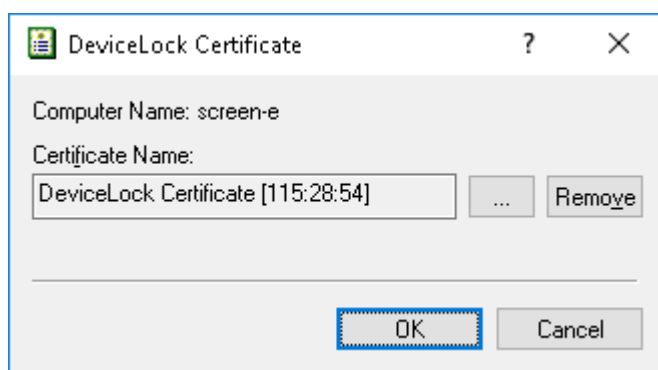
## Log Policy changes and Start/Stop events

You can enable the logging of changes in the DeviceLock Service's configuration and report the time when DeviceLock Service starts and stops. It is possible to log changes in permissions, audit rules, white lists and in other settings.

To enable this kind of logging, enable the **Log Policy changes and Start/Stop events** parameter.

## DeviceLock certificate

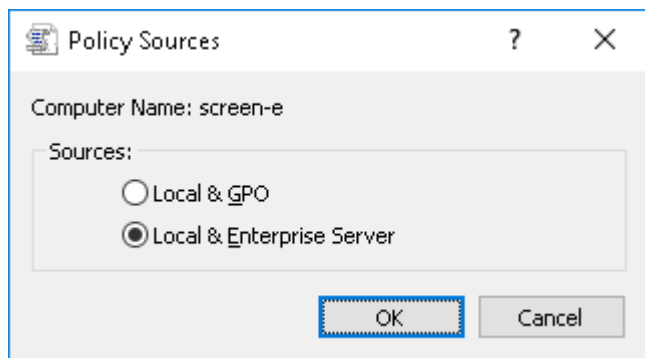
Use this parameter to install or remove the public key of a DeviceLock Certificate.



To install the key, click **...** next to the **Certificate Name** field and specify the file that contains the public key of the desired certificate. To remove the key, click the **Remove** button. For details on DeviceLock certificates, [DeviceLock Certificates](#).

## Policy Source(s)

Use this parameter in conjunction with the parameter [Use Group/Server Policy](#) to specify the source from which DeviceLock Service receives its settings.



You can select one of the following options:

- **Local & GPO** - DeviceLock Service either receives its settings from a Group Policy object or uses locally specified settings, depending upon the parameter [Use Group/Server Policy](#).
- **Local & Enterprise Server** - DeviceLock Service either receives its settings from a DeviceLock Enterprise Server policy object or uses locally specified settings, depending upon the parameter [Use Group/Server Policy](#).

By default, an implicit option of **Any** is used to select the group/server policy source. This option will apply the first received policy - either GPO or Enterprise Server, after which the selection of the policy source will be automatically set - **Local & GPO** or **Local & Enterprise Server**, respectively.

---

### Important

DeviceLock Service can receive its settings from the Acronis cyber protection system. In this case, the **Policy Source(s)** option setting has no effect and you must use the Acronis cyber protection service console to manage DeviceLock Service.

---

## Use Group/Server Policy

When this option is disabled, the local DeviceLock Service settings are in effect. When this option is enabled, the effective settings are determined by Group Policy or DeviceLock Enterprise Server policy depending upon the [Policy Source\(s\)](#) setting.

If the computer is configured to work with Group Policy, the **Use Group/Server Policy** option allows you to choose either Group Policy or Local Policy mode for the DeviceLock Service. Enable this option to choose Group Policy mode. Settings configured using DeviceLock Management Console or DeviceLock Enterprise Manager will be replaced with Group Policy settings. Disable this option to choose Local Policy mode. Settings configured using DeviceLock Management Console or DeviceLock Enterprise Manager will take precedence over Group Policy settings and replace them.

If the computer is configured to work with DeviceLock Enterprise Server policy (see [DeviceLock Enterprise Server Policies](#)), the **Use Group/Server Policy** option allows you to choose either Server

Policy or Local Policy mode for the DeviceLock Service. Enable this option to choose Server Policy mode. Settings configured using DeviceLock Management Console or DeviceLock Enterprise Manager will be replaced with server policy settings. Disable this option to choose Local Policy mode. Settings configured using DeviceLock Management Console or DeviceLock Enterprise Manager will take precedence over server policy settings and replace them.

If the computer is not configured to work with Group Policy or DeviceLock Enterprise Server policy, the **Use Group/Server Policy** option is disabled and cannot be changed.

If the **Use Group/Server Policy** option is enabled and cannot be changed, it means that the Group Policy or Server Policy mode is enforced by enabling the **Override Local Policy** option in DeviceLock Group Policy Manager or in the DeviceLock Enterprise Server policy. A description of this option see in the [Using DeviceLock Group Policy Manager](#) section.

---

### Important

DeviceLock Service can receive its settings from the Acronis cyber protection system. In this case, the **Use Group/Server Policy** option setting has no effect and you must use the Acronis cyber protection service console to manage DeviceLock Service.

---

### Recommendations

When the **Use Group/Server Policy** option is enabled, any local DeviceLock Service settings made using the DeviceLock Management Console will be overwritten with the settings received from outside after a while. Depending on the [Policy Source\(s\)](#) option, the settings may come from a Group Policy Object (GPO) or from the DeviceLock Enterprise Server. It is not possible to use local and external settings at the same time.

Thus, group/server policy and local policy cannot be concurrently applied to the same computer. However, if you want one of the computers to use local settings while the other computers get their settings from the GPO or from the server, you can disable the **Use Group/ Server Policy** option for that specific computer. As a result, the computer will no longer receive its settings from an external source and the local policy will be applied.

If the computer is in the scope of a GPO or has a server policy object applied to it, the console may not allow you to disable the **Use Group/Server Policy** option: the option is enabled and cannot be changed. This is usually caused by the **Override Local Policy** parameter setting in the policy object (see [Using DeviceLock Group Policy Manager](#)). Disable this parameter in the policy object, or remove the computer from the scope of the GPO or from the server policy object. In the case of a GPO, you can move the computer to a different OU in the Active Directory domain where this GPO is not applied. In the case of server policy, follow the instructions in [Changing the Policy Object for a Client Computer](#).

### Fast servers first

DeviceLock Service can choose the fastest available DeviceLock Enterprise Server from the list of servers.

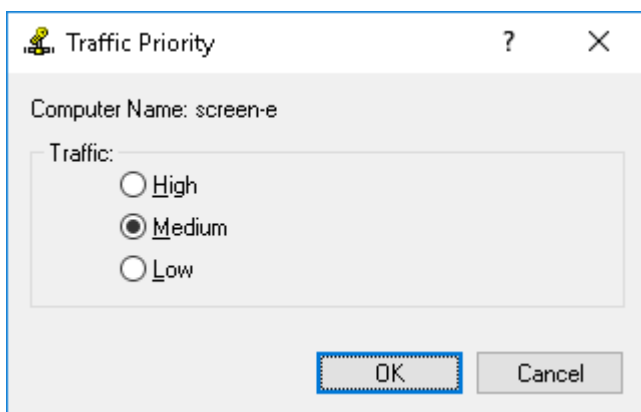
When this parameter is enabled, all servers specified in the **DeviceLock Enterprise Server(s)** parameter are divided into three groups depending on their network speed and preference is given to the fastest. If all of the fastest servers are unavailable, DeviceLock Service attempts to select a server from the group of next fastest servers and so on.

If the **Fast servers first** parameter is disabled, DeviceLock Service randomly selects a server from the list.

This parameter has an effect only if there is more than one server specified in the **DeviceLock Enterprise Server(s)** parameter.

## Traffic priority

DeviceLock supports traffic shaping, allowing you to define network bandwidth limits for sending the audit and shadow logs from DeviceLock Service to DeviceLock Enterprise Server.



In the dialog box that appears when you double-click **Traffic priority**, you can choose from the following options to limit the network bandwidth utilization for transmitting the logs to the server:

- **High** - Do not limit the utilization of the network bandwidth.
- **Medium** - Utilize at most 50% of the network bandwidth.
- **Low** - Utilize at most 20% of the network bandwidth.


---

### Important

Traffic priority options require QoS Packet Scheduler to be enabled on the network connection of the computer running DeviceLock Service. Otherwise, traffic priority cannot be set and DeviceLock Service utilizes the entire available network bandwidth when transferring the logs.

---

## Always show tray icon

Use this option to display or hide the DeviceLock icon in the taskbar notification area (also known as the system tray) of the computer running the DeviceLock Service. When this option is enabled, the DeviceLock icon  appears in the notification area. Disabling this option hides the icon.

The look of the icon depends upon the DeviceLock current operation mode:



- Online mode. The regular profile is used.



- Offline mode. The offline profile is used.



- Determining the current connection state. The previous state profile is used.

When the user moves the mouse pointer over the DeviceLock icon, the following information is displayed:

- DeviceLock version and build number.
- DeviceLock current operation mode (online, offline, or determining), in accordance with the look of the DeviceLock icon.

Clicking the icon displays the most recent DeviceLock notification that appeared on this computer.

When the user right-clicks the DeviceLock icon, the following commands appear:

- **Show Message History** - Display all notifications since the last start-up of the DeviceLock Service.
- **Refresh Current State** - Determine the current connection state and choose the operation mode accordingly.
- **DeviceLock Applet** - Open the DeviceLock applet that can be used to:
  - Obtain temporary access to a device (see [Temporary White List Authorization Tool](#)).
  - Load a signed file with new settings (see [Loading signed settings file on Windows](#)).

To display or hide the DeviceLock icon, right-click the option **Always show tray icon** and then click **Enable** or **Disable**, or double-click that option.

## Archives content inspection on read

Use this option to enable or disable content inspection of files within archives when users try to read archive files. For details, see the [Inspection of files within archives](#) feature description. To enable or disable content inspection of files within archives, right-click **Archives content inspection on read** and then click **Enable/Disable**, or double-click **Archives content inspection on read**.

---

### Note

- If this option is enabled, a failure may occur upon inspecting a password-protected file (archive, PDF or Microsoft Office document) because the content to check cannot be extracted from that file. In this case, DeviceLock will block transferring the file due to a content inspection failure.
  - If this option is disabled, inspection of documents embedded in saved emails (EML), Adobe Portable Document Format (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx) is also not performed.
- 

## Archives content inspection on write

Use this option to enable or disable content inspection of files within archives when users try to write archive files. For details, see the [Inspection of files within archives](#) feature description. To enable or disable content inspection of files within archives, right-click **Archives content**

**inspection on write** and then click **Enable/Disable**, or double-click **Archives content inspection on write**.

---

**Note**

- If this option is enabled, a failure may occur upon inspecting a password-protected file (archive, PDF or Microsoft Office document) because the content to check cannot be extracted from that file. In this case, DeviceLock will block transferring the file due to a content inspection failure.
  - If this option is disabled, inspection of documents embedded in saved emails (EML), Adobe Portable Document Format (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx) is also not performed.
- 

## Binary Files Content Inspection

The **Binary Files Content Inspection** option allows for inspecting text content held in arbitrary binary files. When this option is disabled, DeviceLock performs keywords- and text pattern-based content analysis for only Unicode text held in certain file types (the file types listed in [Expansive coverage of multiple file formats and data types](#) in the [ContentLock and NetworkLock](#) section).

When this option is enabled, DeviceLock performs keywords- and text pattern-based content analysis for text held in any binary files, regardless of text encoding (Unicode or non-Unicode). In this case, content inspection may take considerably longer to complete.

---

**Note**

This option affects content-aware rules that employ keywords groups, pattern groups and/or complex content groups containing those group types. For details regarding content-aware rules, see [Content-Aware Rules \(Regular Profile\)](#).

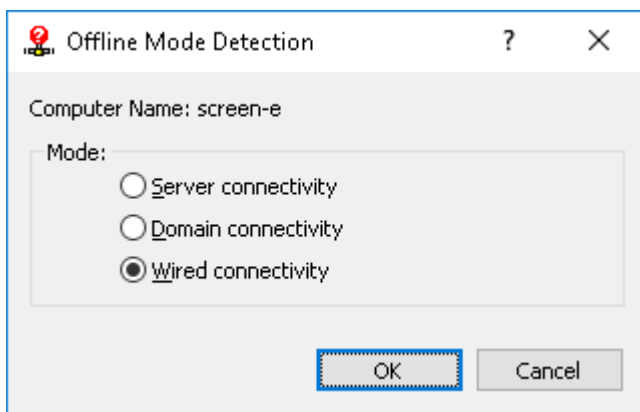
---

To enable or disable this option, double-click the **Binary Files Content Inspection** item in the **Service Options** list, or right-click that item and then choose **Enable** or **Disable**.

## Offline mode detection

Use this option to configure offline mode detection settings. You can define the network characteristics that DeviceLock uses to detect its connection state (whether it is online or offline). By default, DeviceLock works in offline mode when the network cable is not connected to the client computer.

To configure offline mode detection settings, right-click **Offline mode detection** and then click **Properties**, or double-click **Offline mode detection**.



You can choose from the following options:

- **Server connectivity** - The connection state is determined by whether the DeviceLock Service logs can be transferred from the client computer to DeviceLock Enterprise Server. When this option is selected, the computer is considered to work in online mode if the server can receive DeviceLock logs for at least one of the users who are currently using that computer. The server is determined by the [DeviceLock Enterprise Server\(s\)](#) setting in [Service Options](#). The computer is considered to work in offline mode if the server cannot receive DeviceLock logs for any one of the users who are currently using that computer. This may occur because the DeviceLock Service is unable to authenticate to any designated DeviceLock Enterprise Server or all designated servers are unavailable.
- **Domain connectivity** - The connection state is determined by whether a connection can be established to a controller of the Active Directory domain to which the client computer belongs. When this option is selected, the computer is considered to work in online mode if it is connected to a controller of its domain. The computer is considered to work in offline mode if it cannot connect to any controller of its domain or it is not joined to a domain.
- **Wired connectivity** - The connection state is determined by whether the network cable is plugged into the Network Interface Card (NIC) of the client computer. This is the simplest and least secure method of detecting the connection state. When this option is selected, the computer is considered to work in online mode if the network cable is plugged into its NIC. The computer is considered to work in offline mode if the network cable is unplugged. Please note that only cable connections are taken into account. Wireless network connections (Wi-Fi, etc.) and modem connections are disregarded.

---

**Note**

DeviceLock certificate-based authentication provides the most reliable way to secure client/ server communication. For client/server certificate authentication, the public key must be installed on client computers, while the private key must be installed on DeviceLock Enterprise Server/s.

If the certificate's public key is installed only on client computers, the server will reject connections and client computers will work in offline mode. If the certificate's private key is installed only on the DeviceLock Enterprise Server, the server and the client will authenticate each other once a connection is established although this type of authentication is less secure than client/server certificate authentication. For details on DeviceLock certificates, see [DeviceLock Certificates](#).

---

For more information and instructions on how to manage DeviceLock policies for offline mode, see [DeviceLock Security Policies \(Offline Profile\)](#).

## OWA server(s)

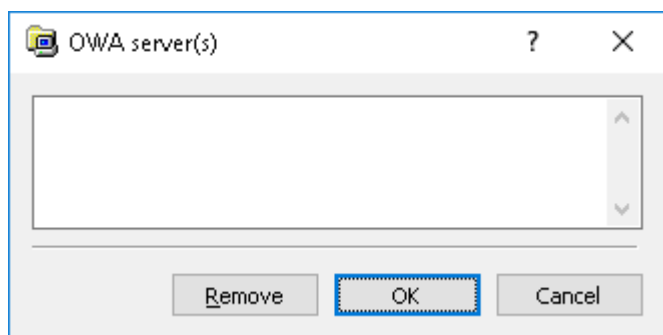
This parameter allows you to define the list of Outlook Web App (OWA, formerly Outlook Web Access) server's URLs. The OWA servers specified here are treated as the Web Mail protocol by the NetworkLock module. All OWA servers not specified here are treated as the HTTP protocol by the NetworkLock module. This parameter requires that the NetworkLock policy (any protocols-related DeviceLock parameters) be defined. Otherwise, this parameter has no effect.

---

**Note**

The outlook.office.com and outlook.office365.com servers are always treated as the OWA servers.

---



Multiple URLs must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry. You can use the asterisk (\*) wildcard in URLs (for example, \*.com/owa matches any URL that ends in .com/owa).

## Apply Content-Aware Rules to file/folder names

Use this option to enable or disable the inspection of file and folder names using content-aware rules. When you enable this option, consider the following:

- Only rules based on Pattern and Keywords groups apply to file and folder names.
- The rules apply to the file's full path, including the file name and all folder names.



- The rules trigger when reading, writing or transferring files through devices or protocols that have content-aware rules specified.
- If content-aware rules have not been specified for a particular file-related action, then this option has no effect when performing that action.

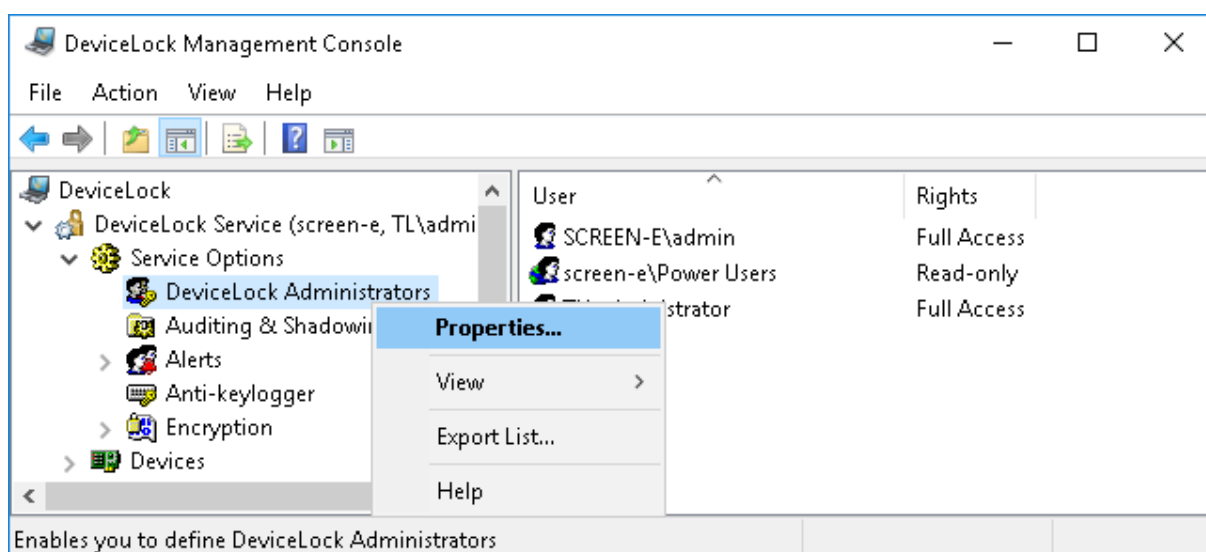
## EtherSensor Server

In the dialog box for this setting, specify the name of the computer running the EtherSensor server. This can be a short name, a fully-qualified domain name or IP address of the computer. Provide the number of the EtherSensor port next to the computer name, in the following format: computer name [port number]. Example: MyServer[8080]

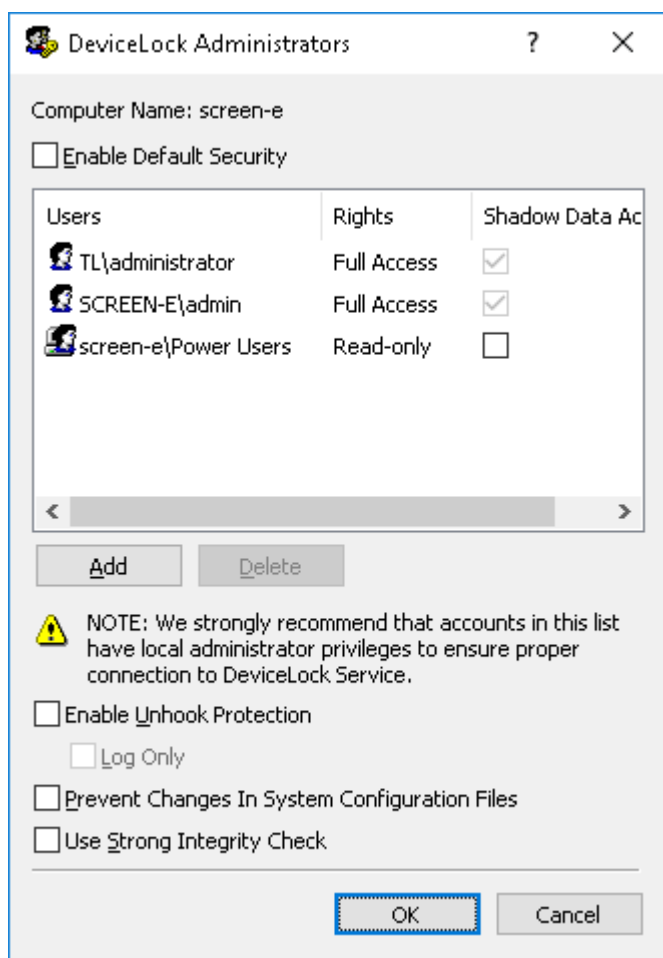
This setting enables DeviceLock to associate users with application-level data objects (messages, files, etc.) intercepted by EtherSensor. With this setting, EtherSensor can recognize on the network the objects related to users of the computer running the DeviceLock Service. For more information about EtherSensor, see [deviceclock.com/products/network-hybrid-dlp.html](https://deviceclock.com/products/network-hybrid-dlp.html).

## DeviceLock Administrators

This parameter allows you to define the list of user accounts with administrative access rights to DeviceLock Service.



Click **Properties** on the shortcut menu of the **DeviceLock Administrators** item to open the configuration dialog box.



DeviceLock's default security configuration is based on Windows Access Control Lists (ACL). A user without administrative privileges can't connect to DeviceLock Service, modify its settings or remove it. Everything is controlled by the Windows security subsystem.

To turn on the Windows ACL-based security, select the **Enable Default Security** check box.

### Note

As described in the [Basic Security Rules](#) section of this manual, giving administrative privileges to regular users is strongly discouraged.

Users with local administrator privileges (i.e. members of the local Administrators group) can connect to DeviceLock Service using a management console and change permissions, auditing and other parameters. Moreover, such users can uninstall DeviceLock from their computers, disable or delete DeviceLock Service, modify a service's registry keys, delete a service's executable file, and so on. In other words, users with local administrator privileges can circumvent the default security based on Windows ACL.

However, if for some reason, users in your network have administrator privileges on their local computers, DeviceLock does provide another level of protection - DeviceLock Security. When DeviceLock Security is enabled, no one except authorized users can connect to DeviceLock Service

or stop and uninstall it. Even members of the local Administrators group (if they are not on the list of authorized DeviceLock administrators) can't circumvent DeviceLock Security.

To turn on DeviceLock Security, clear the **Enable Default Security** check box.

Then you need to specify authorized accounts (users and/or groups) that can administer DeviceLock Service. To add a new user or user group to the list of accounts, click the **Add** button. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using Ctrl and/or Shift you can highlight and remove several records simultaneously.

To determine the actions allowed to a user or group, select the desired level of access:

- **Full access** - Allows the user or group to modify permissions, auditing and other parameters, remove and update DeviceLock Service.
- **Change** - Allows the user or group to change settings, install, and uninstall DeviceLock Service. Unlike full access, does not give the right to make changes to the list of DeviceLock administrators or change access rights for existing users or groups in that list.
- **Read-only** - Only allows the user or group to view permissions, auditing and other parameters. Users can view defined parameters but cannot modify anything or remove/update DeviceLock Service.

For users and groups with **Change** or **Read-only** access, the **Shadow Data Access** option can be selected to allow access to shadow copies and user activity records. The users and groups with this option selected are allowed to open, view, and save shadow copies and user activity records from DeviceLock Service logs by using Shadow Log Viewer (see [Shadow Log Viewer \(Service\)](#)) and UAM Log Viewer (see [Viewing User Activity](#)).

---

#### Note

Without access to shadow data, DeviceLock Service administrators do not have access to the content of shadow copies and user activity records. They cannot open, view, or save shadow copies and records of user activity.

---

We strongly recommend that DeviceLock Service administrators be given local administrator rights as installing, updating, and uninstalling DeviceLock Service may require access rights to Windows Service Control Manager (SCM) and shared network resources.

Consider the following recommendation to properly define the list of DeviceLock administrators: Add the Domain Admins group with **Full access** rights to this list. Since the Domain Admins group is a member of the Administrators local group on every computer in the domain, all members of Domain Admins will have full access to the DeviceLock Service on every computer. However, other members of the Administrators local group will not be able to administer the DeviceLock Service or disable it.

Select the **Enable Unhook Protection** check box to turn on protection against anti-rootkits that might be maliciously used to disable the DeviceLock Service. With this protection turned on, any attempt to violate the integrity of the DeviceLock code will cause a fatal error in Windows (BSOD).

---

**Note**

Some antivirus, firewall and other low-level third-party software may conflict with the unhook protection and cause fatal errors (BSOD). We recommend that you enable this protection only for the systems where it was tested before.

---

If you select the **Log Only** check box, DeviceLock does not cause Windows to stop with a fatal error (BSOD) when a violation is found. Instead, the event about this violation is written into the audit log.

Select the **Prevent Changes In System Configuration Files** check box to instruct DeviceLock Service to automatically secure the Windows Hosts file.

---

**Note**

Because DeviceLock uses the local Hosts file for host name resolution, a malicious user with local administrator rights can modify the Hosts file as required to bypass DeviceLock security policies. In order to minimize security risks, we recommend that you secure the Hosts file using the **Prevent Changes In System Configuration Files** option.

---

Also, by selecting or clearing the **Use Strong Integrity Check** check box, you can specify the type of integrity checks to use. You can run two types of integrity checks to detect corruption in DeviceLock Service's executable files:

- Simple integrity check: DeviceLock Service checks version information of all its executable files. To specify this type of integrity checks, clear the **Use Strong Integrity Check** check box.
- Strong integrity check: DeviceLock Service verifies the digital signatures of all its executable files. To specify this type of integrity checks, select the **Use Strong Integrity Check** check box. A strong integrity check requires more time than a simple integrity check.

**Recommendations**

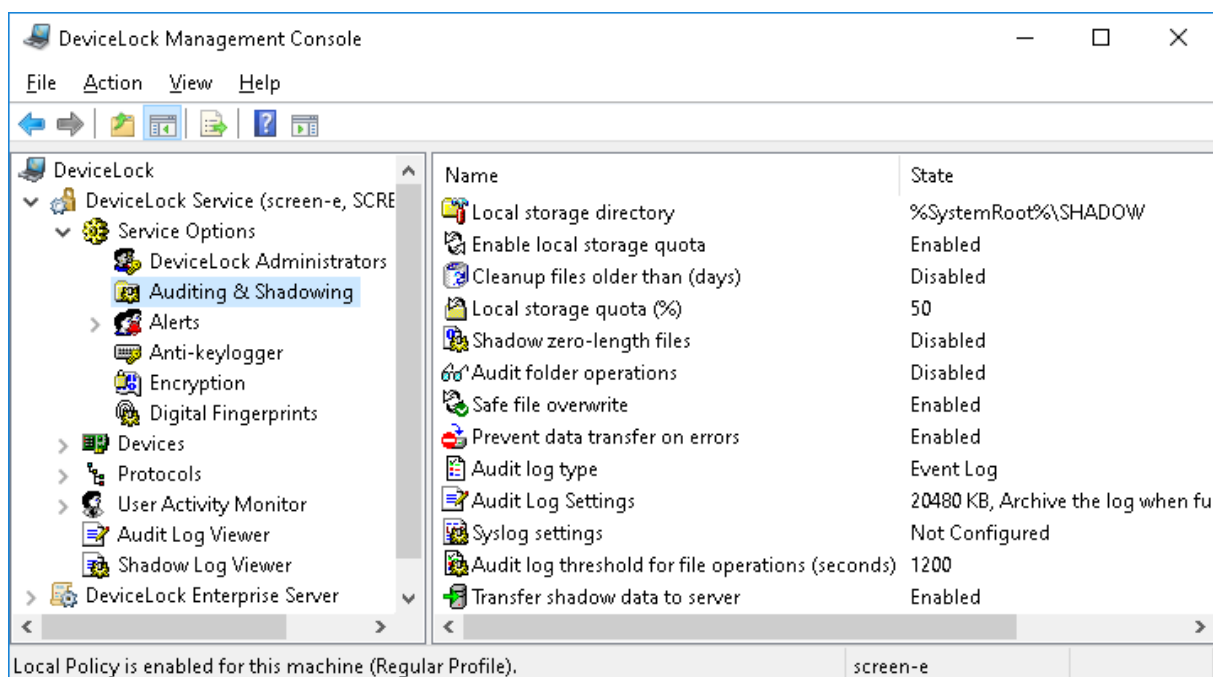
With default security disabled and a list of DeviceLock Administrators set up, access to network drives and physical ports on the client computer might be unexpectedly blocked regardless of the effective access permissions. A side effect is that Task Manager does not list the DeviceLock Service process (dlservice).

This behavior is part of the protection against administrators who have full access to the client computer but are not included in the list of DeviceLock administrators. If the DeviceLock Service unexpectedly stops, this protection feature blocks access to the channels of possible data leaks.

Restart the computer to restore DeviceLock access settings. If the problem reappears, try disabling the antivirus software that could force the DeviceLock Service to stop.

## Auditing & Shadowing

These parameters allow you to tune up auditing and shadowing for DeviceLock Service.



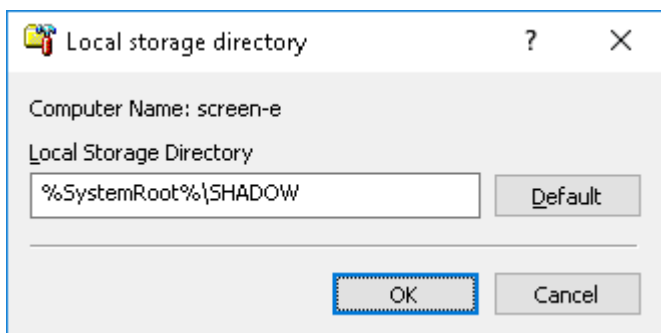
Use the shortcut menu available via a right mouse click on every parameter.

The auditing and shadowing parameters are as follows:

- [Local storage directory](#)
- [Audit log threshold for file operations \(seconds\)](#)
- [Enable local storage quota](#)
- [Cleanup files older than \(days\)](#)
- [Local storage quota \(%\)](#)
- [Shadow zero-length files](#)
- [Audit folder operations](#)
- [Safe file overwrite](#)
- [Prevent data transfer on errors](#)
- [Audit log type](#)
- [Audit log settings](#)
- [Syslog settings](#)
- [Transfer shadow data to server](#)

## Local storage directory

Use this parameter to define where on the local disk cached data (audit/shadowing data, data for content analysis and the alert queue) is stored.



By default, DeviceLock Service uses the %SystemRoot%\SHADOW directory to store cached data (audit/shadowing data, data for content analysis and the alert queue) on the local computer.

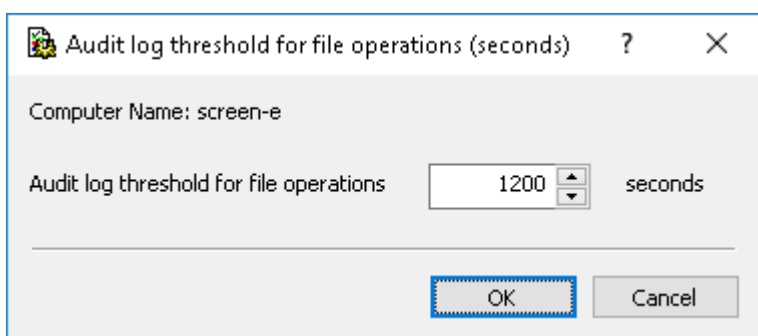
%SystemRoot% is a standard environment variable that expands to a path to the Windows root folder (for example, C:\Windows). You can specify any other directory on any locally accessible hard disk.

DeviceLock Service protects this directory so regular users cannot access files inside it.

Make sure that there is enough space to store the data (if the user copies 1GB to the flash drive, then you need approximately 2GB available in local storage).

### Audit log threshold for file operations (seconds)

You can specify the time threshold, in seconds, used for aggregation of repetitive events associated with file operations.



The default value is 1200 seconds. After this amount of time passes without new repetitive events being recorded, multiple repetitive events are combined into a single summary event if all of the following conditions are true:

- The events are associated with the same user.
- The events are associated with the same process.
- The events are associated with the same file operation (such as read, write, etc.) on a file.

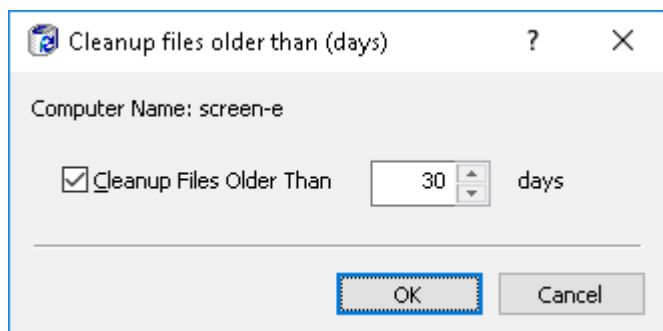
### Enable local storage quota

Enable this parameter to allow automatic cleanup of the locally stored cached data (for shadowing and content analysis).

When this parameter is enabled you can also configure [Cleanup files older than \(days\)](#) and [Local storage quota \(%\)](#) parameters.

## Cleanup files older than (days)

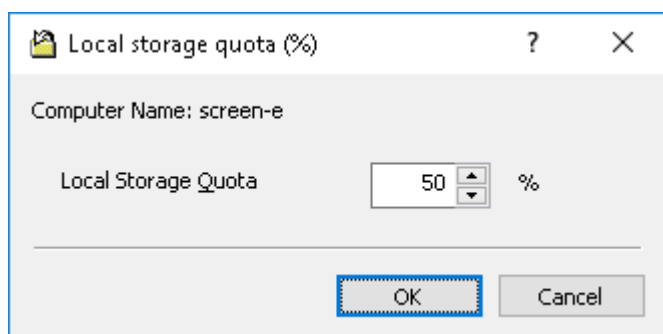
You can define the number of days that should pass before cached data (for shadowing and content analysis) can be automatically deleted from the local storage.



Select the **Cleanup Files Older Than** check box and type or select the number of days to allow automatic cleanup.

## Local storage quota (%)

You can define a disk quota for cached data such as audit data, shadow copies, user activity monitor recordings, file and message content analysis data, and alert queue data.



In the **Local Storage Quota** field, specify the maximum percentage (from 5 to 100) of free disk space that can be allocated for cached data.

If the quota is not set (i.e. the [Enable local storage quota](#) parameter is disabled), the DeviceLock Service uses all available space on the disk specified in the [Local storage directory](#) parameter.

When the size of the folder set by the [Local storage directory](#) parameter exceeds the quota, the DeviceLock Service either starts deleting old data (if the [Cleanup files older than \(days\)](#) option is enabled) or stops data shadowing and content analysis (if the [Cleanup files older than \(days\)](#) option is disabled or there is nothing to delete). When the quota is exceeded, monitoring of user activity also suspends.

## Shadow zero-length files

Enable this parameter to allow shadowing of files whose size is zero.

Even if the file contains no data at all, it is still possible to transfer some information in its name and path (up to several kilobytes) that is why you may need to enable shadowing for zero-length files.

## Audit folder operations

Enable this parameter to turn on the audit logging of events associated with operations on folders, such as creating (writing), renaming, reading (opening), and deleting folders. When this parameter is disabled, all events associated with folder operations will be excluded from auditing.

## Safe file overwrite

Enable this parameter to prevent the deletion of the original file as a result of user attempts to replace it with a file with the same name and prohibited contents. When this parameter is enabled, the original file remains in the folder intact once its overwriting is prohibited by content-aware rules. The event of the original file restoration is logged in the audit log.

---

### Note

When this parameter is enabled and any content-aware rules are in effect that deny write access, deletion of files may take longer than usual.

---

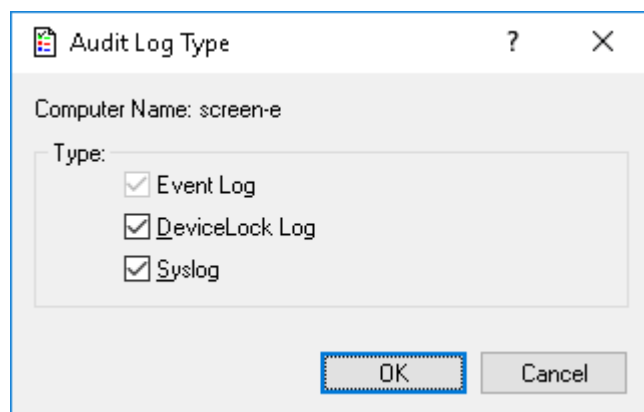
## Prevent data transfer on errors

Enable this parameter to prevent users from transferring data when shadowing or content analysis is not possible. As a result, users will only be able to transfer data if the disk has sufficient space to store shadow copies and to save the data that is necessary for the normal functioning of Content-Aware Rules.

When the **Prevent data transfer on errors** parameter is enabled, the total size of the directory specified in [Local storage directory](#) reaches the quota specified in [Local storage quota \(%\)](#), and there is no data that can be deleted, the DeviceLock Service stops shadowing and content analysis, and blocks any user data transfer attempts.

## Audit log type

Using this parameter you can define what logs should be used to store audit records.



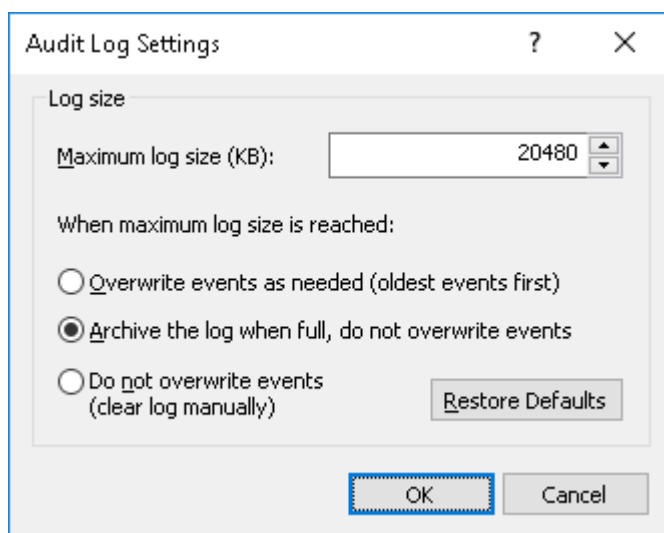
There are three options to choose:



- **Event Log** - The standard local Windows Event Log is used to store audit records.
- **DeviceLock Log** - The protected proprietary log is used to store audit records. The data from this log is sent to DeviceLock Enterprise Server and is stored centrally in the database.
- **Syslog** - Audit records are sent to the syslog server.

## Audit log settings

Use **Audit log settings** to specify the maximum size of the audit log and overwrite options.

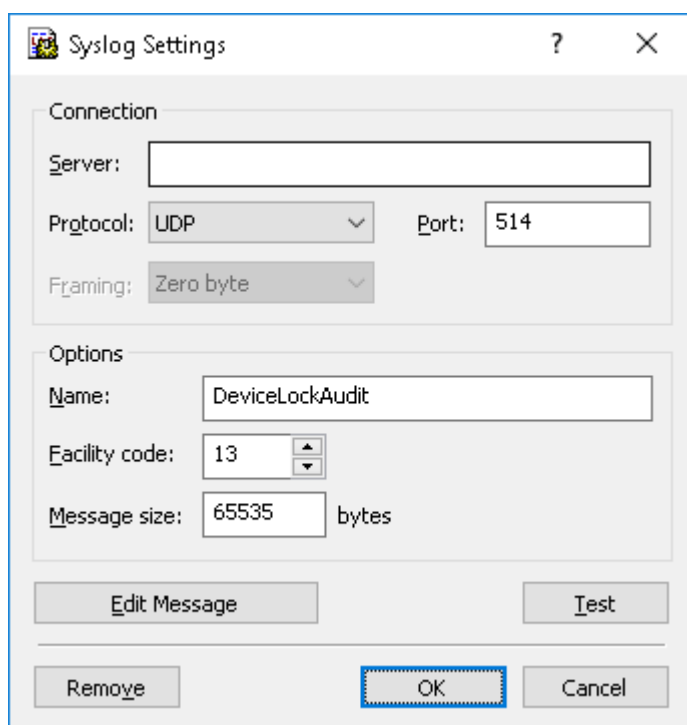


The screenshot shows the 'Audit Log Settings' dialog box. It has a title bar with a question mark and a close button. The main area is titled 'Log size' and contains a text box for 'Maximum log size (KB)' with the value '20480'. Below this, there is a section 'When maximum log size is reached:' with three radio button options: 'Overwrite events as needed (oldest events first)', 'Archive the log when full, do not overwrite events' (which is selected), and 'Do not overwrite events (clear log manually)'. There is a 'Restore Defaults' button next to the third option. At the bottom, there are 'OK' and 'Cancel' buttons.

For details on the audit log settings, see [Audit Log Settings \(Service\)](#).

## Syslog settings

Use **Syslog settings** to configure syslog forwarding.

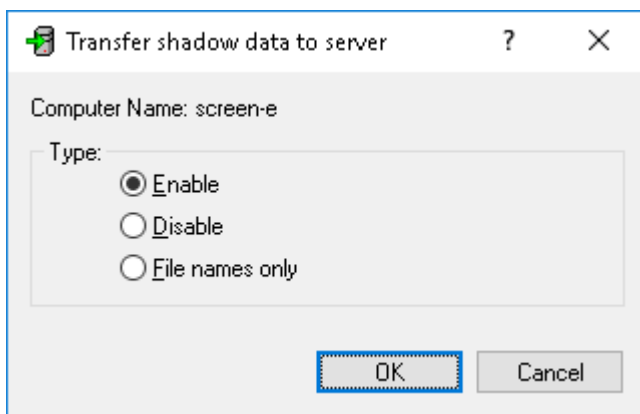


The screenshot shows the 'Syslog Settings' dialog box. It has a title bar with a question mark and a close button. The main area is divided into two sections: 'Connection' and 'Options'. The 'Connection' section has a 'Server:' text box, a 'Protocol:' dropdown menu set to 'UDP', a 'Port:' text box with the value '514', and a 'Framing:' dropdown menu set to 'Zero byte'. The 'Options' section has a 'Name:' text box with the value 'DeviceLockAudit', a 'Facility code:' dropdown menu set to '13', and a 'Message size:' text box with the value '65535' followed by the text 'bytes'. At the bottom, there are buttons for 'Edit Message', 'Test', 'Remove', 'OK', and 'Cancel'.

- **Connection** - Supply the following information:
  - **Server** - The IP address or fully qualified domain name of the syslog server.
  - **Protocol** - Either **TCP** or **UDP** as the method of communication with the syslog server. The default selection is **UDP**.
  - **Port** - The port number on which to send syslog messages. The default value is 514.
  - **Framing** - The framing method for syslog messages when transported over TCP. DeviceLock supports these methods: **Zero byte**, **LF**, **CR+LF**, **Message length**.
- **Options** - Specify the following options:
  - **Name** - A unique name for the log channel. The default name is **DeviceLockAudit**.
  - **Facility code** - A syslog standard value (between 0 and 23) to specify the type of program that is logging the message.
  - **Message size** - The syslog message size, in bytes. The default value is **65535** bytes.
- **Edit Message** - Customize the predefined contents of the syslog message for audit based on the template described in [Alerts Settings: Syslog](#).  
In the **Syslog Message for Audit** dialog box that opens you can also do the following:
  - Select the message severity level using **Level** drop-down menu.
  - Load the specified message body from a tab-delimited text file (.txt). To do so, click **Load**. The entire contents of the file are loaded.
  - Restore the default settings. To do so, click **Restore Defaults**.
- **Remove** - Remove all syslog settings.
- **Test** - Send a test syslog message to verify that DeviceLock Service is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:
  - The test can complete successfully, meaning that a test message was successfully sent using the configured syslog parameters. The resulting message states: "Test Syslog audit was successfully sent."
  - The test can fail, meaning that a test message was not sent. The resulting message states: "Test Syslog audit was not sent due to error: <error\_description>."

## Transfer shadow data to server

Use this parameter to configure the transfer of shadow copy data and [User Activity Monitor](#) sessions to DeviceLock Enterprise Server.



There are three options to choose from:

- **Enable** - All shadow copy data and User Activity Monitor session recordings are transferred to DeviceLock Enterprise Server.
- **Disable** - All shadow copy data and User Activity Monitor session recordings are stored on the client computer without transferring them to DeviceLock Enterprise Server. Only audit data from the DeviceLock proprietary log (if this log is used) is transferred to DeviceLock Enterprise Server.
- **File names only** - Shadow file names, rather than entire files, are transferred to DeviceLock Enterprise Server. Shadow files are stored locally on the client computer, and can later be transferred to DeviceLock Enterprise Server by selecting the **Enable** option for the **Transfer shadow data to server** parameter.

With the **File names only** option, information about User Activity Monitor sessions is transferred to the server whereas the session recordings are not. The recordings are stored on the client computer, and can be transferred later by selecting the **Enable** option for the **Transfer shadow data to server** parameter.

---

### Important

If shadow file names only are transferred to the server and then files are removed to the Deleted Shadow Data Log, then, upon selecting the **Enable** option for the **Transfer shadow data to server** parameter, the following behavior occurs: Those files are not transferred to the server and they are deleted from the client computer.

---

## Alerts

You can define alerts to automatically notify you of significant incidents, events or problems when they occur. Real-time alerting simplifies event monitoring and log management and helps you response faster and more efficiently to security incidents and policy violations.

DeviceLock supports the following types of alerts:

- Alerts that are generated when a specific user attempts to access a specific device type or a protocol.
- Alerts that are generated when a specific Content-Aware Rule fires.
- Alerts that are generated when a specific firewall rule fires.

- Administrative alerts. Some examples of administrative alerts include “Notify if Service settings are changed”; “Notify if Service settings are corrupted” and many others.

Alerts can be sent to their intended recipients through e-mail or SNMP traps. Also, alerts can be sent to a syslog server.

Before DeviceLock can send alert notifications, you should do the following:

- Decide how to be notified when alert conditions occur: through SNMP traps, e-mail, or syslog.
- To be notified through SNMP traps, configure DeviceLock Service for SNMP support and specify the SNMP server to send traps to (see [Alerts Settings: SNMP](#)).

---

**Note**

This manual assumes a basic understanding of the Simple Network Management Protocol (SNMP) and related network management concepts.

---

- To be notified through e-mail, configure e-mail notifications by specifying SMTP Server and e-mail notification settings and defining the e-mail templates (see [Alerts Settings: SMTP](#)).
- To be notified through syslog, configure DeviceLock Service for syslog and specify the syslog server to send alerts to (see [Alerts Settings: Syslog](#)).

---

**Note**

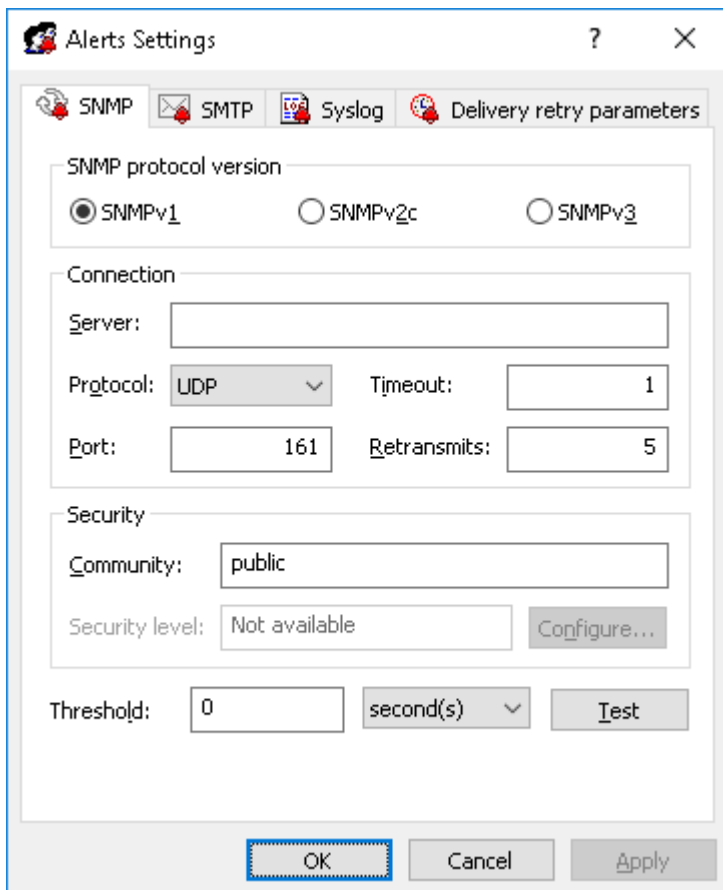
This manual assumes a basic understanding of syslog and related message logging concepts.

---


- Configure alert delivery failure parameters such as the delivery retry count, delivery retry interval, and the amount of time an undelivered notification is kept in the queue for delivery (see [Alerts Settings: Delivery retry parameters](#)).
- Enable notifications for specific events. When you enable notifications for specific events, you specify the conditions for which you want to be notified. For information on how to enable administrative alerts, see [Administrative Alerts](#). For information on how to enable device type-specific alerts, see [Auditing, Shadowing & Alerts \(Regular Profile\)](#). For information on how to enable protocol-specific alerts, see [Managing Audit, Shadowing and Alerts for Protocols](#). For information on how to enable alerts for a specific Content-Aware Rule, see [Defining Rules for Devices](#) and [Defining Rules for Protocols](#). For information on how to enable alerts for a specific firewall rule, see [Managing Basic IP Firewall](#) and [Defining firewall rules](#).

## Alerts Settings: SNMP

Use the **SNMP** tab in the **Alerts Settings** dialog box to configure DeviceLock Service for SNMP support.



To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.
- Select **Alerts** in the console tree, and then click **Manage**  on the toolbar.
- Select **Alerts** in the console tree; then, in the details pane, right-click **SNMP** and click **Manage**.
- Select **Alerts** in the console tree, and then double-click **SNMP** in the details pane.

### Note

You can define different online vs. offline alert settings. Online alert settings (Regular Profile) apply to client computers that are working online. Offline alert settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#).

DeviceLock supports SNMPv1, SNMPv2c, and SNMPv3 protocols. You can configure DeviceLock Service to automatically send alert notifications to the specified SNMP server when alert conditions occur. These alerts are sent only when all of the following conditions are met:

- The SNMP server is set up to receive traps.
- The remote computer running the SNMP server is accessible from all computers running DeviceLock Service.
- Alerts have been configured to be sent through SNMP traps.

Complete the **SNMP** tab as follows:

- **SNMP protocol version** - Configure DeviceLock Service to use the version of SNMP supported by the SNMP server. Available options are: **SNMPv1**, **SNMPv2c**, and **SNMPv3**.
- **Connection** - Configure the SNMP server information.
  - **Server** - Specify the SNMP sever to send traps to. To do so, in the **Server** box, type the SNMP server host name or IP address.
  - **Protocol** - Specify the transport protocol for passing data between DeviceLock Service and the SNMP server. Available options are: **UDP** and **TCP**.
  - **Timeout** - Specify the time (in seconds) that DeviceLock Service waits for the SNMP server to reply before retransmitting the data packet. The default value is 1 second.
  - **Port** - Specify the port on which the SNMP server listens for traps. The default value is 161.
  - **Retransmits** - Specify the number of times DeviceLock Service's request is re-sent to the SNMP server, if the server is not responding. The default value is 5.  
*This value is set only for TCP connections.*
- **Security** - Configure SNMP security settings:
  - **Community** - Specify the SNMP community string to use for authentication with the SNMP server. The default value is `public`. Applicable only to SNMPv1 and SNMPv2c.
  - **Security user name** - Specify the user account to use for authentication with the SNMP server. Applicable only to SNMPv3. If authentication is not required, no authentication credentials need to be specified.
  - **Context name** - Specify the context name if an SNMP context is configured on the SNMP server. Applicable only to SNMPv3.
  - **Context engine ID** - Specify the context engine ID if an SNMP context is configured on the SNMP server. Applicable only to SNMPv3.
  - **Authentication protocol** - Specify the protocol used to encrypt the authentication with the SNMP server. Applicable only to SNMPv3. Available options:
    - **None** - Corresponds to the SNMP security level **No security**. Communication without authentication and without privacy.
    - **HMAC-SHA** - Corresponds to the SNMP security level **Authentication**.
  - **Password/Confirm password** - Specify the password corresponding to the user account to use for authentication with the SNMP server. Applicable only to SNMPv3.
  - **Privacy protocol** - Specify the protocol used to encrypt data for SNMP communication. Applicable only to SNMPv3. Available options:
    - **None** - Corresponds to the SNMP security level **No security**. Communication with authentication and without privacy.
    - **CBC-AES-128** - Corresponds to the SNMP security level **Authentication and Privacy**. Communication with authentication and privacy.
  - **Password/ Confirm password** - Specify the password for data encryption (privacy). Applicable only to SNMPv3.

- **Threshold** - Specify the time interval (in hours, minutes and seconds) used for event aggregation when generating alerts. DeviceLock Service aggregates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:
  - a. The events are of the same type (**Success**, **Failure**, or **Information**).
  - b. The events are associated with the same device type/protocol.
  - c. The events are associated with the same user.
  - d. The events are associated with the same PID.
 The default value is 0 seconds.

---

#### Note

DeviceLock Service aggregates only access-related events when generating alerts. Administrative events are not aggregated.

---

- **Test** - Send a test SNMP trap to verify that DeviceLock Service is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:
  - The test can complete successfully, meaning that a test SNMP trap was successfully sent using the configured SNMP trap parameters. The resulting message states: "Test SNMP alert was successfully sent."
  - The test can fail, meaning that a test SNMP trap was not sent. The resulting message states: "Test SNMP alert was not sent due to error: <error description>."

SNMP traps by DeviceLock Service are presented in the Management Information Base (MIB) format. MIB for DeviceLock Service has the object identifier (OID) 1.3.6.1.4.1.60000 or iso.org.dod.internet.private.enterprise.DeviceLock, and it contains the following branch nodes:

- products(1)
- agent(1)
- alerts(1) - This node contains the following single MIB objects:
  - eventType(1) - The class of an event: Success for allowed access, Failure for denied access, or Information for events generated by Content-Aware rules of Detection type. Note that the value of eventType is displayed as a numeric value instead of a text string: 8 indicates success, 16 indicates failure, and 4 indicates information.
  - eventId(2) - A number identifying the particular event type.
  - userSid(3) - The security identifier (SID) of the user associated with this event.
  - userName(4) - The name of the user associated with this event.
  - computerName(5) - The name of the computer from which the event was received.
  - processId(6) - The identifier of the process associated with this event.
  - processName(7) - The name of the process associated with this event.
  - source(8) - The type of device or protocol involved. Please note that the value of source is displayed as a numeric value rather than a text string. The following numeric values are used:

Devices	Protocols
1 - Floppy	513 - ICQ Messenger
2 - Removable	514 - HTTP
3 - Hard disk	515 - Torrent
5 - Optical Drive	516 - FTP
7 - Serial port	517 - SMTP
8 - Parallel port	520 - Jabber
9 - Tape	521 - IRC
10 - USB port	522 - Telnet
11 - Infrared port	524 - Mail.ru Agent
12 - FireWire port	525 - Web Mail
13 - Bluetooth	526 - Social Networks
14 - WiFi	527 - SSL
15 - Windows Mobile	528 - SMB
16 - Palm	529 - MAPI
17 - Printer	530 - File Sharing
18 - iPhone	531 - Skype
19 - BlackBerry	533 - Any (TCP)
20 - Clipboard	534 - Any (UDP)
21 - TS Devices	539 - IP (TCP)
22 - MTP	540 - IP (UDP)
	541 - IBM Notes
	542 - WhatsApp
	546 - Telegram
	547 - Viber
	548 - Tor Browser
	549 - Web Search
	550 - Career Search
	551 - Zoom



- action(9) - The user's activity type.
- name(10) - The name of the object (file, USB device, etc.).
- info(11) - Other device-specific information for the event, such as the access flags, device names, and so on.
- reason(12) - The cause of the event.
- datetime(13) - The date and time (in the RFC3339 date/time format) when the event was received by DeviceLock Service.

---

## Note

These MIB objects correspond to audit log fields.

---

A trap is sent just once each time an event associated with an alert occurs. Below is an example of the SNMP alert.

☐ Specific: 1

- Message reception date: 12.09.2012
- Message reception time: 12:55:27.466
- Time stamp: 244 days 08h:34m:52s.24th
- Message type: Trap (v1)
- Protocol version: SNMPv1
- Transport: IP/UDP
- ☐ Agent
  - Address: 10.10.30.15
  - Port: 62562
- ☐ Manager
  - Address: [10.10.30.16](#)
  - Port: 0
- Community: public
- SNMPv1 agent address: 10.10.30.15
- Enterprise: enterprises.60000
- ☐ Bindings (13)
  - Binding #1: enterprises.60000.1.1.1.1 \*\*\* (gauge) 16
  - Binding #2: enterprises.60000.1.1.1.2 \*\*\* (gauge) 13
  - Binding #3: enterprises.60000.1.1.1.3 \*\*\* (octet string) S-1-5-21-3601177953-2830843172-1403898981-500
  - Binding #4: enterprises.60000.1.1.1.4 \*\*\* (octet string) \win7x64\Administrator
  - Binding #5: enterprises.60000.1.1.1.5 \*\*\* (octet string) \WIN7X64
  - Binding #6: enterprises.60000.1.1.1.6 \*\*\* (gauge) 456
  - Binding #7: enterprises.60000.1.1.1.7 \*\*\* (octet string) C:\Windows\Explorer.EXE
  - Binding #8: enterprises.60000.1.1.1.8 \*\*\* (gauge) 2
  - Binding #9: enterprises.60000.1.1.1.9 \*\*\* (octet string) \write
  - Binding #10: enterprises.60000.1.1.1.10 \*\*\* (octet string) E:\Market research.docx
  - Binding #11: enterprises.60000.1.1.1.11 \*\*\* (octet string) (zero-length)
  - Binding #12: enterprises.60000.1.1.1.12 \*\*\* (octet string) Rule: "Confidential data" (Any keyword matched)
  - Binding #13: enterprises.60000.1.1.1.13 \*\*\* (octet string) 2012-09-12T08:55:26Z


## Alerts Settings: SMTP

Use the **SMTP** tab in the **Alerts Settings** dialog box to configure e-mail notifications.

The image shows the 'Alerts Settings' dialog box with the 'SMTP' tab selected. The dialog has four tabs: 'SNMP', 'SMTP', 'Syslog', and 'Delivery retry parameters'. The 'SMTP' tab contains the following sections:

- Connection:** Includes 'SMTP host:' and 'Port:' (set to 25).
- Security:** Includes a checkbox for 'Server requires authentication', 'User name:', and a 'Password...' button.
- Options:** Includes 'Sender address:' and 'Recipients addresses:' text boxes.
- Buttons:** 'Edit Message' and 'Edit Admin. Message'.
- Threshold:** A numeric input set to 10, a unit dropdown set to 'minute(s)', and a 'Test' button.
- Footer:** 'OK', 'Cancel', and 'Apply' buttons.

To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.
- Select **Alerts** in the console tree, and then click **Manage**  on the toolbar.
- Select **Alerts** in the console tree; then, in the details pane, right-click **SMTP** and click **Manage**.
- Select **Alerts** in the console tree, and then double-click **SMTP** in the details pane.

### Note

You can define different online vs. offline alert settings. Online alert settings (Regular Profile) apply to client computers that are working online. Offline alert settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#).

DeviceLock uses the Simple Mail Transfer Protocol (SMTP) for e-mail messaging. You can configure DeviceLock Service to automatically send notifications to the specified e-mail address or addresses when alert conditions occur. To configure e-mail notifications, you must do the following:

1. Specify SMTP server and e-mail notification settings.
2. Define the e-mail templates.

DeviceLock comes with ready-to-use e-mail message templates that you can use to define the message content. These templates determine the basic content, format, and structure of e-mail notifications. DeviceLock provides the following templates:

- An e-mail message for administrative alerts.
- An e-mail message for all other alerts.

Each e-mail template contains the following information:

- **Message subject** - The text used in the **Subject** line of the e-mail message. The default message subject for administrative alerts is "DeviceLock Administrative Alert". The default message subject for all other alerts is "DeviceLock Alert".
- **Message body** - The text used in the body of the e-mail message. DeviceLock can send either the plain text body or an HTML version of the message body. The message body is the same in both templates and includes static text and macros. The default static text in the message body is "The following event has occurred". You can use the following predefined macros to insert additional information in the **Subject** line and/or the body of the e-mail message:
  - %EVENT\_TYPE% - The class of event: **Success** for allowed access, **Failure** for denied access, or **Information** for administrative events.
  - %COMP\_NAME% - The name of the computer from which the event was received.
  - %COMP\_FQDN% - The fully-qualified domain name of the computer from which the event was received.
  - %COMP\_IP% - The comma-delimited list of all network addresses (IPs) associated with the computer.
  - %DATE\_TIME% - The date and time when the event was received by DeviceLock Service. The date and time are displayed based on the client computer's regional and language settings.
  - %SOURCE% - The type of device or protocol involved.
  - %ACTION% - The user's activity type.
  - %NAME% - The name of the object (file, USB device, etc.).
  - %INFO% - Other device-specific information for the event, such as the access flags, device names, and so on.
  - %REASON% - The cause of the event.
  - %USER\_NAME% - The name of the user associated with this event.
  - %USER\_SID% - The security identifier (SID) of the user associated with this event.
  - %PROC\_NAME% - The name of the process associated with this event.
  - %PROC\_ID% - The identifier of the process associated with this event.
  - %EVENT\_ID% - The number identifying the particular event type.
  - %SUMMARY\_TABLE% - A table detailing individual events for aggregated alerts.

*These macros are replaced with their actual values at the message generation time.*

Complete the **SMTP** tab as follows:

- **Connection** - Configure the e-mail server connection information for notification e-mails.
  - **SMTP host** - Specify the SMTP server host name or IP address.
  - **Port** - Specify the port number through which e-mail is sent to your e-mail server. The default port is 25.

---

#### Note

Both non-SSL (unencrypted) and SSL connections to the specified SMTP server are supported. DeviceLock automatically identifies encrypted connections and their type.

---

- **Security** - Set the SMTP security options.
  - **Server requires authentication** - Specify the type of authentication to use with the SMTP server. Select the **Server requires authentication** check box to specify basic authentication. Clear the **Server requires authentication** check box to specify no authentication.
  - **User name** - Specify the user name to use for authentication with the SMTP server. This property requires a value if you specified basic authentication.
  - **Password/ Confirm password** - Specify the password to use for authentication with the SMTP server. This property requires a value if you specified basic authentication.
- **Options** - Define the e-mail sender and recipients.
  - **Sender address** - Specify the e-mail address from which the alerts will be sent.
  - **Recipients addresses** - Specify the e-mail addresses of e-mail recipients (those who will receive the e-mail notification of events). Multiple e-mail addresses must be separated by a comma (,) or semicolon (;).
- **Edit Message** - Customize the predefined contents of the e-mail message for alerts based on the template.

In the **E-mail Message for Alerts** dialog box that opens you can also do the following:

  - Change the message format for all messages to HTML or plain text. To do so, click either **Text** or **HTML**. By default, e-mail messages are sent in plain text format.
  - Load the specified message body from a tab-delimited text file (.txt). To do so, click **Load**. The entire contents of the file are loaded. The text can be either plain text or HTML as needed.
  - Restore the default settings. To do so, click **Restore Defaults**.
- **Edit Admin. Message** - Customize the predefined contents of the e-mail message for administrative alerts based on the template.

In the **E-mail Message for Administrative Alerts** dialog box that opens you can also do the following:

  - Change the message format for all messages to HTML or plain text. To do so, click either **Text** or **HTML**. By default, e-mail messages are sent in plain text format.
  - Load the specified message body from a tab-delimited text file (.txt). To do so, click **Load**. The entire contents of the file are loaded. The text can be either plain text or HTML as needed.
  - Restore the default settings. To do so, click **Restore Defaults**.

- **Threshold** - Specify the time interval (in hours, minutes and seconds) used for event consolidation when generating alerts. DeviceLock Service consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:
  - a. The events are of the same type (**Success**, **Failure**, or **Information**).
  - b. The events are associated with the same device type/protocol.
  - c. The events are associated with the same user.
  - d. The events are associated with the same PID.The default value is 10 minutes.

---

**Note**

DeviceLock Service combines only access-related events when generating alerts.  
Administrative events are not consolidated.

---

- **Test** - Send a test e-mail notification to verify that DeviceLock Service is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:
  - The test can complete successfully, meaning that a test e-mail notification was successfully sent using the configured e-mail notification parameters. The resulting message states: "Test SMTP alert was successfully sent."
  - The test can fail, meaning that a test e-mail notification was not sent. The resulting message states: "Test SMTP alert was not sent due to error: <error description>."

Below is an example of the e-mail alert.

**DeviceLock Alert**

The following event has occurred:

Event type: Failure (16)

Computer: WIN7X64

Date/Time: 09/11/12 18:24:38

Source: Removable (2)

Action: Write

Name: E:\Market research.docx

Info:

Reason: Rule: "Confidential data" (Matched: All keywords)

User name: Win7x64\Administrator

User SID: S-1-5-21-3601177953-2830843172-1403898981-500

Process name: C:\Windows\Explorer.EXE

Process Id: 456

Event id: 13

---

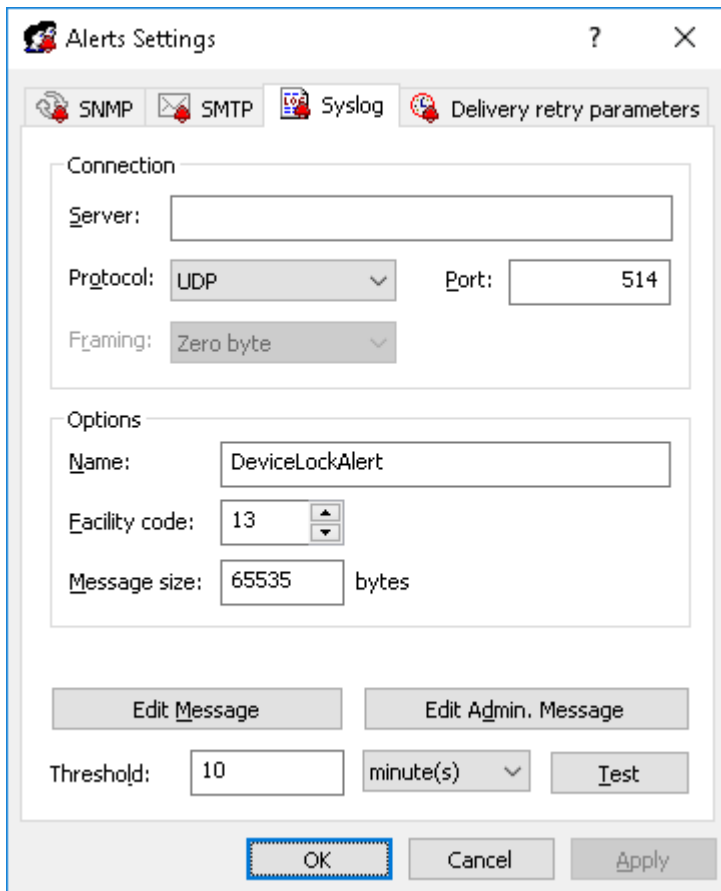
**Note**

Field names in an e-mail alert correspond to field names in the Audit Log.

---

## Alerts Settings: Syslog

Use the **Syslog** tab in the **Alerts Settings** dialog box to configure DeviceLock Service for syslog.



The image shows the 'Alerts Settings' dialog box with the 'Syslog' tab selected. The dialog has four tabs: SNMP, SMTP, Syslog, and Delivery retry parameters. The 'Syslog' tab is active, showing configuration options for syslog alerts. The 'Connection' section includes fields for 'Server', 'Protocol' (set to UDP), 'Port' (set to 514), and 'Framing' (set to Zero byte). The 'Options' section includes fields for 'Name' (set to DeviceLockAlert), 'Facility code' (set to 13), and 'Message size' (set to 65535 bytes). At the bottom, there are buttons for 'Edit Message', 'Edit Admin. Message', 'Threshold' (set to 10), a unit dropdown (set to minute(s)), a 'Test' button, and 'OK', 'Cancel', and 'Apply' buttons at the very bottom.

Alerts Settings

SNMP SMTP Syslog Delivery retry parameters

Connection

Server:

Protocol: UDP Port: 514

Framing: Zero byte

Options

Name: DeviceLockAlert

Facility code: 13


Message size: 65535 bytes

Edit Message Edit Admin. Message

Threshold: 10 minute(s) Test

OK Cancel Apply

To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.
- Select **Alerts** in the console tree, and then click **Manage**  on the toolbar.
- Select **Alerts** in the console tree; then, in the details pane, right-click **Syslog** and click **Manage**.
- Select **Alerts** in the console tree, and then double-click **Syslog** in the details pane.

---

### Note

You can define different online vs. offline alert settings. Online alert settings (Regular Profile) apply to client computers that are working online. Offline alert settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#).

---

You can configure DeviceLock Service to automatically send alert notifications to the specified syslog server when alert conditions occur. These alerts are sent only when all of the following conditions are met:

- The syslog server is set up to receive messages.
- The remote computer running the syslog server is accessible from all computers running DeviceLock Service.
- Sending alerts to the syslog server is configured.

DeviceLock comes with ready-to-use syslog message templates. These templates determine the basic content, format, and structure of notifications. DeviceLock provides the following templates:

- A syslog message for administrative alerts.
- A syslog message for all other alerts.

Each template contains the following information:

- **Message body** - The text used in the body of syslog message. The message body is the same in both templates and includes static text and macros. The default static text in the message body is "The following event has occurred". You can use the following predefined macros to insert additional information in the body of the syslog message:
  - %EVENT\_TYPE% - The class of event: **Success** for allowed access, **Failure** for denied access, or **Information** for administrative events.
  - %COMP\_NAME% - The name of the computer from which the event was received.
  - %COMP\_FQDN% - The fully-qualified domain name of the computer from which the event was received.
  - %COMP\_IP% - The comma-delimited list of all network addresses (IPs) associated with the computer.
  - %DATE\_TIME% - The date and time when the event was received by DeviceLock Service. The date and time are displayed based on the client computer's regional and language settings.
  - %SOURCE% - The type of device or protocol involved.
  - %ACTION% - The user's activity type.
  - %NAME% - The name of the object (file, USB device, etc.).
  - %INFO% - Other device-specific information for the event, such as the access flags, device names, and so on.
  - %REASON% - The cause of the event.
  - %USER\_NAME% - The name of the user associated with this event.
  - %USER\_SID% - The security identifier (SID) of the user associated with this event.
  - %PROC\_NAME% - The name of the process associated with this event.
  - %PROC\_ID% - The identifier of the process associated with this event.
  - %EVENT\_ID% - The number identifying the particular event type.
  - %SUMMARY\_TABLE% - A table detailing individual events for aggregated alerts.

*These macros are replaced with their actual values at the message generation time.*

Complete the **Syslog** tab as follows:

- **Server** - Specify the IP address or fully qualified domain name of the syslog server.
- **Protocol** - Select **TCP** or **UDP** as the method of communication with the syslog server. The default selection is **UDP**.
- **Port** - Specify the port number on which to send syslog messages. The default value is 514.
- **Framing** - Specify the framing method for syslog messages when transported over TCP. DeviceLock supports these methods: **Zero byte**, **LF**, **CR+LF**, **Message length**.
- **Name** - Specify the unique name for the log channel. The default name is **DeviceLockAlert**.
- **Facility code** - Select a syslog standard value (between 0 and 23) to specify the type of program that is logging the message.
- **Message size** - Specify the syslog message size, in bytes. The default size is 65535 bytes.
- **Edit Message** - Customize the predefined contents of the syslog message for alerts based on the template.

In the **Syslog Message for Alerts** dialog box that opens you can also do the following:

- Select the message severity level using **Level** drop-down menu.
  - Load the specified message body from a tab-delimited text file (.txt). To do so, click **Load**. The entire contents of the file are loaded.
  - Restore the default settings. To do so, click **Restore Defaults**.
- **Edit Admin. Message** - Customize the predefined contents of the syslog message for administrative alerts based on the template.
- In the **Syslog Message for Administrative Alerts** dialog box that opens you can also do the following:
- Select the message severity level using **Level** drop-down menu.
  - Load the specified message body from a tab-delimited text file (.txt). To do so, click **Load**. The entire contents of the file are loaded.
  - Restore the default settings. To do so, click **Restore Defaults**.
- **Threshold** - Specify the time interval (in hours, minutes and seconds) used for the aggregation of events when generating alerts. DeviceLock Service combines multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:
    - a. The events are of the same type (**Success**, **Failure**, or **Information**).
    - b. The events are associated with the same device type/protocol.
    - c. The events are associated with the same user.
    - d. The events are associated with the same PID.
 The default value is 10 minutes.

---

#### Note

DeviceLock Service combines only access-related events when generating alerts. Administrative events are not aggregated.

---

- **Test** - Send a test syslog message to verify that DeviceLock Service is configured correctly. This test operation can have two different outcomes, each resulting in a different message being

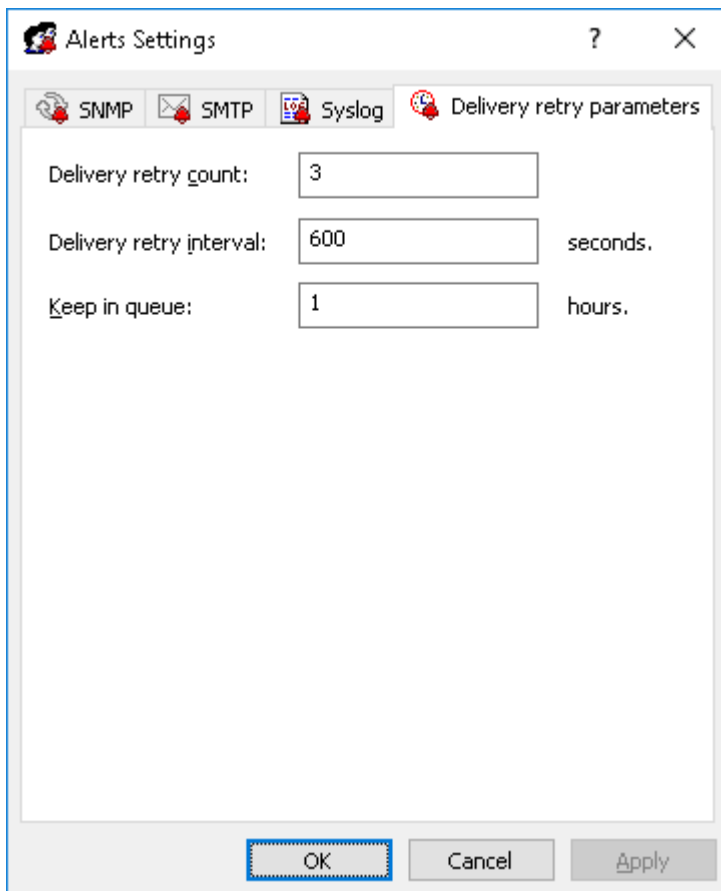


displayed:


- The test can complete successfully, meaning that a test message was successfully sent using the configured syslog parameters. The resulting message states: "Test Syslog alert was successfully sent."
- The test can fail, meaning that a test message was not sent. The resulting message states: "Test Syslog alert was not sent due to error: <error description>."

## Alerts Settings: Delivery retry parameters

Use the **Delivery retry parameters** tab in the **Alerts Settings** dialog box to configure DeviceLock Service actions in case of alert delivery failure.



To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.
- Select **Alerts** in the console tree, and then click **Manage**  on the toolbar.
- Select **Alerts** in the console tree; then, in the details pane, right-click **Delivery retry parameters** and click **Manage**.
- Select **Alerts** in the console tree, and then double-click **Delivery retry parameters** in the details pane.

---

**Note**

You can define different online vs. offline alert settings. Online alert settings (Regular Profile) apply to client computers that are working online. Offline alert settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#).

---

DeviceLock generates and delivers alerts the moment the alert conditions are met. If alerts cannot be delivered on the first try, DeviceLock creates a queue to store undelivered alerts for a specified amount of time and sends them again. You can specify the maximum number of times DeviceLock attempts to send an alert, set the interval between delivery tries and also define the amount of time undelivered alerts are kept in the queue for delivery.

Complete the **Delivery retry parameters** tab as follows:

- **Delivery retry count** - Specify the maximum number of times DeviceLock attempts to send an alert if the first delivery attempt fails. If the first delivery attempt fails, the alert is deferred to the queue and marked as having had one delivery attempt. Thereafter, each time the queued alert is sent and delivery fails, the number of attempts is incremented.

This parameter must contain a value between 0 and 999. The default value is 3.

When the delivery retry count is reached and delivery fails, DeviceLock logs an error in the Audit Log ("`<channel name>` for alerts is unavailable and temporary disabled due to error: `<error code>` - `<error description>`") and temporarily stops further transmissions through the alert delivery channel (SNMP, SMTP and/or syslog).

DeviceLock will automatically attempt to re-establish connection with the specified SNMP, SMTP, or syslog server when checking its connection state (whether it is online or offline, see [Switching Between Online and Offline Mode](#) for details). If the connection is restored, DeviceLock resumes sending alerts.

Different values of this parameter are used for regular and offline profiles.

- **Delivery retry interval: seconds** - Specify how many seconds DeviceLock waits before it attempts next delivery of the alert, if the previous delivery failed. This parameter must contain a value between 10 and 3600. The default value is 600 seconds.
- **Keep in queue: hours** - Define the amount of time in hours undelivered alerts are kept in the queue for delivery before they are deleted. The same queue is used for all delivery channels (SNMP, SMTP and/or syslog).

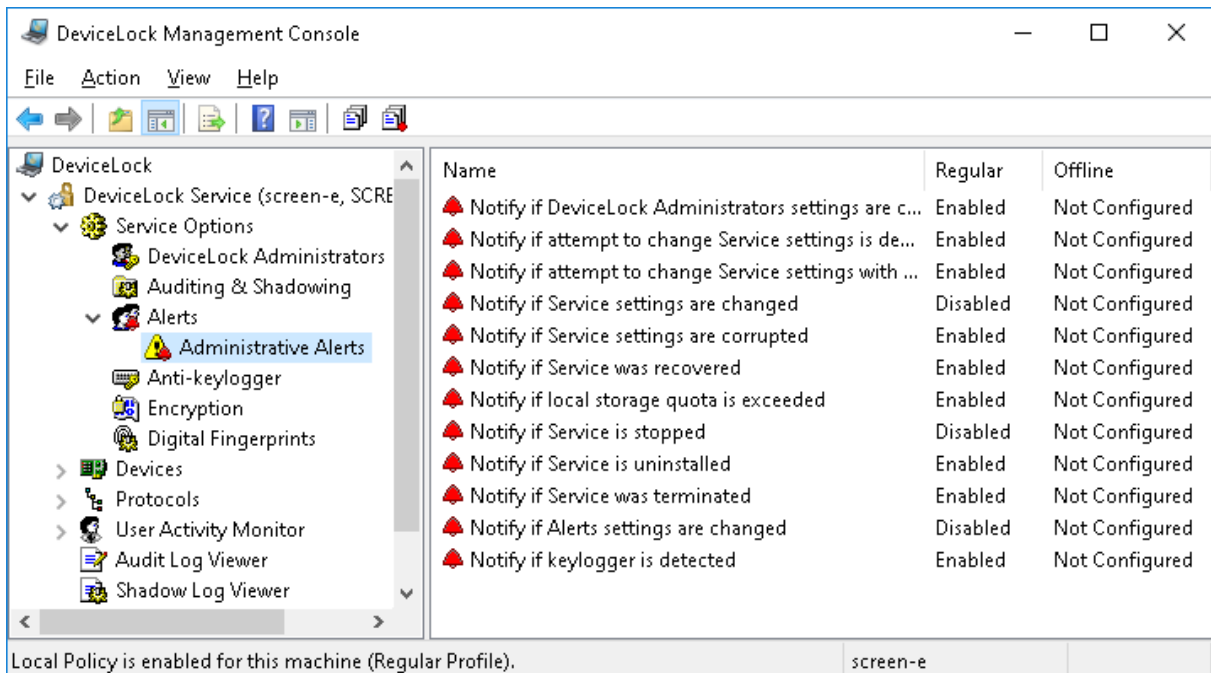
This parameter must contain a value between 1 and 999. The default value is 1 hour.

This parameter can be specified only for the regular profile. The same value of this parameter is used for both profiles (regular and offline).

## Administrative Alerts

You can enable administrative alerts to automatically notify you of critical events, requiring direct administrator actions. Once enabled, an alert will be sent to the specified destinations when such a critical event is encountered.

When you select **Administrative Alerts** in the console tree, the details pane lists administrative alerts that you can enable or disable.



In the details pane, right-click any alert to display a shortcut menu that contains the following commands:

- **Enable** - Enables the online (regular) administrative alert.
- **Disable** - Disables the online (regular) administrative alert.
- **Undefine** - Returns the regular administrative alert to the unconfigured state. Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.
- **Enable Offline** - Enables the offline administrative alert.
- **Disable Offline** - Disables the offline administrative alert.
- **Undefine Offline** - Returns the previously defined offline administrative alert to the unconfigured state. If offline administrative alerts are undefined, regular administrative alerts are applied to offline client computers.
- **Manage** - Opens a dialog box where you can configure regular administrative alerts collectively.
- **Manage Offline** - Opens a dialog box where you can configure offline administrative alerts collectively.
- **Remove Offline** - Blocks the inheritance of offline administrative alerts and enforces regular administrative alerts. Available only in DeviceLock Group Policy Manager and DeviceLock Service Settings Editor.

---

**Note**

You can enable different online vs. offline administrative alerts. Online alerts (Regular Profile) are generated when client computers are working online. Offline alerts (Offline Profile) are generated when client computers are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#).

---

Available administrative alerts include:

- **Notify if DeviceLock Administrators settings are changed** - DeviceLock sends this notification when any changes have been made to the DeviceLock Administrators settings. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.
- **Notify if attempt to change Service settings is denied** - DeviceLock sends this notification when DeviceLock Security is enabled and a user with insufficient access rights attempts to modify DeviceLock Service settings multiple times over a short period. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.
- **Notify if attempt to change Service settings with enabled "Override Local Policy" is denied** - DeviceLock sends this notification when the **Override Local Policy** parameter is enabled in DeviceLock Group Policy Manager and any user that connected DeviceLock Management Console to the computer running DeviceLock Service attempts to modify the service's settings. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.
- **Notify if Service settings are changed** - DeviceLock sends this notification when one or more DeviceLock Service settings (except for DeviceLock Administrators settings) have been modified. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the type of device or protocol involved, the user's activity type, the type of the profile, the name of the user, the user's SID, and the event ID.
- **Notify if Service settings are corrupted** - DeviceLock sends this notification when DeviceLock Service starts and detects corruption of its settings. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.  
*DeviceLock Service uses a checksum calculation to validate its settings. All corrupted settings are automatically restored.*
- **Notify if Service was recovered** - DeviceLock sends this notification when the DeviceLock Driver starts and detects removal of one or more DeviceLock Service installation files. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.

*All missing files are automatically restored.*

- **Notify if local storage quota is exceeded** - DeviceLock sends this notification when the local storage quota for audit/shadowing data, the alert queue, and data for content analysis has been exceeded. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the user, the user's SID, and the event ID.  
For detailed information on the local storage quota, see [Local storage quota \(%\)](#) parameter description.
- **Notify if Service is stopped** - DeviceLock sends this notification when DeviceLock Service starts after it has been stopped. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the version number of DeviceLock Service, the name of the user, the user's SID, and the event ID.
- **Notify if Service is uninstalled** - DeviceLock sends this notification when DeviceLock Service is uninstalling. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the version number of DeviceLock Service, the name of the user, the user's SID, and the event ID.
- **Notify if Service was terminated** - DeviceLock sends this notification when DeviceLock Service restarts after incorrect termination. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the version number of DeviceLock Service, the name of the user, the user's SID, and the event ID.
- **Notify if Alerts settings are changed** - DeviceLock sends this notification when one or more alert settings have been modified. The notification is sent according to the previous alert settings. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the type of the profile, the name of the user, the user's SID, the identifier of the process associated with this event, and the event ID.
- **Notify if keylogger is detected** - DeviceLock sends this notification when hardware USB keylogger is detected. The notification will include such information as the type of the event, the name of the computer, the date and time when the event was received, the user's activity type, the name of the USB device detected as a keylogger, the name of the user, the user's SID, and the event ID. The [Log event](#) parameter in **Anti-keylogger** options should be enabled to allow this notification. For more information, refer to the [Anti-keylogger](#) section of this manual.



### ***Managing Administrative Alerts***

Administrative alerts can be enabled individually or collectively.

To enable online (regular) or offline administrative alerts individually, right-click any Administrative Alert, and then click **Enable** or **Enable Offline**. The Administrative Alert changes its online/offline state from "Not Configured" to "Enabled."

Once you have enabled a particular Administrative Alert, you can disable it. To do so, right-click the enabled Administrative Alert, and then click **Disable** or **Disable Offline**. The Administrative Alert changes its state from “Enabled” to “Disabled”.

You can also disable or enable an online (regular) alert by double-clicking it.

To enable online (regular) or offline administrative alerts collectively, right-click any Administrative Alert, and then click **Manage** or **Manage Offline**. Alternatively, you can select any Administrative Alert, and then click **Manage**  or **Manage Offline**  on the toolbar. Next, in the dialog box that opens, select the appropriate check boxes for the administrative alerts that you want to enable. Once you have enabled Administrative alerts, you can disable them. To do so, clear the appropriate check boxes.

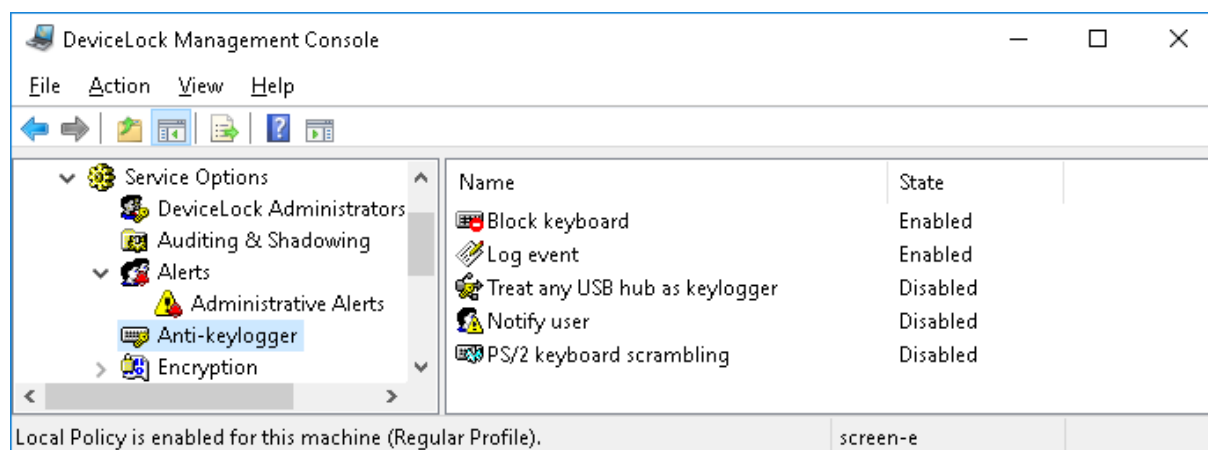
### Note

All check boxes in the **Administrative alerts (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of administrative alerts.

## Anti-keylogger

These parameters allow you to tune up DeviceLock’s ability to detect hardware keyloggers and to define what DeviceLock Service should do when a keylogger is found.

Hardware keyloggers are devices that record keystrokes. DeviceLock Service can detect USB keyloggers and block keyboards connected to them. Also, DeviceLock Service can block PS/2 keyloggers.



Use the shortcut menu available via a right mouse click on every parameter.

The anti-keylogger parameters are as follows:

- [Block keyboard](#)
- [Log event](#)
- [Treat any USB hub as keylogger](#)

- [Notify user](#)
- [PS/2 keyboard scrambling](#)

## Block keyboard

Enable this parameter to block the keyboard connected to the hardware USB keylogger when it is detected.

Since DeviceLock Service starts before the user logs in to Windows, it can block the keyboard and prevent the user from typing the password.

---

### Note

Some hardware keyloggers continue to record keystrokes even if the keyboard is blocked and not functioning in Windows. This happens because such keyloggers are standalone devices and do not require any OS or drivers.

---

## Log event

You can instruct DeviceLock Service to write an event to the audit log when the hardware USB keylogger is detected.

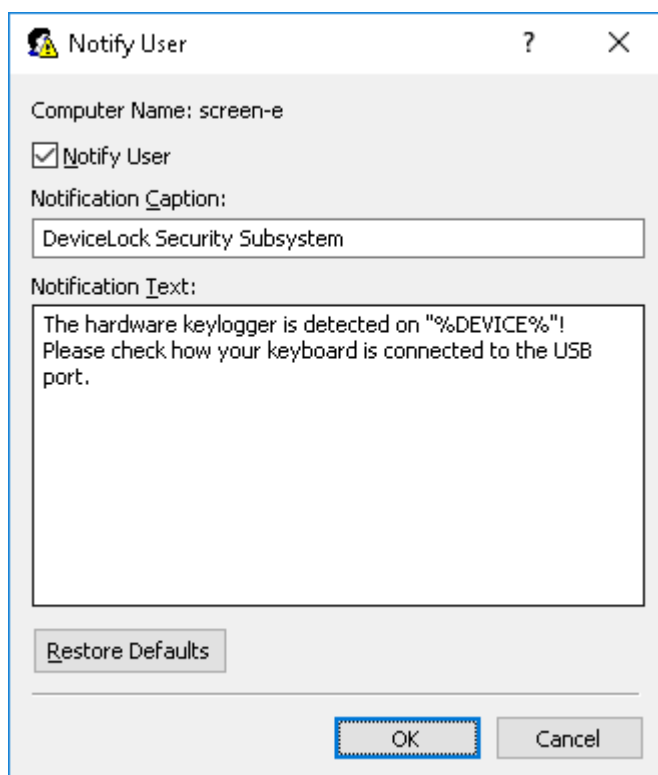
## Treat any USB hub as keylogger

By enabling this parameter, you can instruct DeviceLock Service to treat any external USB hub to which the keyboard is connected as a hardware keylogger.

Otherwise, DeviceLock Service detects only those hub keyloggers that exist in its internal database.

## Notify user

You can define a custom message to be displayed to users when DeviceLock Service detects hardware USB keyloggers.



Since DeviceLock Service starts before the user logs in to Windows, this message can alert the user and prevent him/her from typing the password on the keyboard connected to the USB keylogger.

To enable this custom message, select the **Notify User** check box.

Also, you can define additional parameters, such as:

- **Notification Caption** - The text to be displayed as a caption. You can use the predefined macros within the text:
  - **%DEVICE%** - Inserts the name of the keyboard's device (for example, USB Keyboard) received from the system.
- **Notification Text** - The main text of the message. You can use the predefined macros described above within the text.

## PS/2 keyboard scrambling

By enabling this parameter, you can prevent PS/2 keyloggers from recording keystrokes. DeviceLock Service is unable to detect PS/2 keyloggers and notify users about their presence but it obfuscates PS/2 keyboard's input and forces PS/2 keyloggers (if any) to record some garbage instead of the real keystrokes.

---

### Note

When PS/2 keyboard scrambling is enabled while working with the PS/2 KVM switch, the switching between computers will not work from the keyboard.

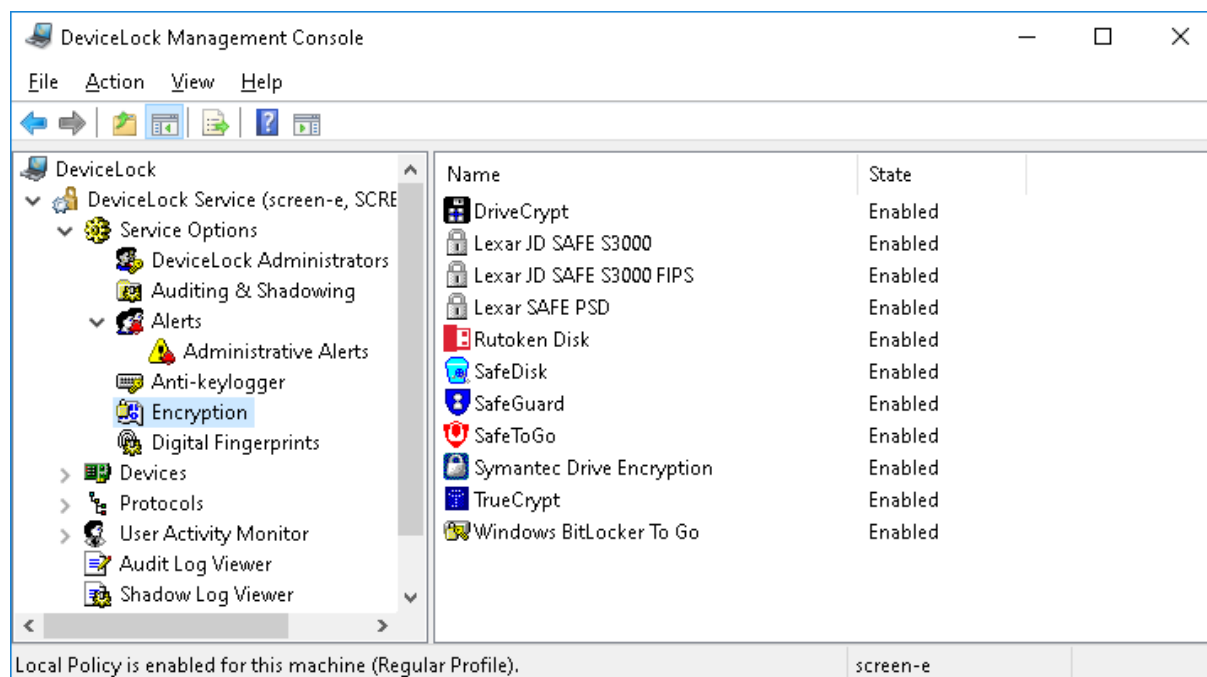
---



## Encryption

DeviceLock Service can recognize disks (USB-drives and other removable devices) that store data in an encrypted form, and apply so-called “encrypted” permissions for such disks (see [“Encrypted” Rights Category](#)). This feature makes it possible to prevent sensitive data from being written to media that does not provide encryption.

The encryption products and technologies that DeviceLock supports are listed in the details pane when **DeviceLock Service > Service Options > Encryption** is selected in the console tree:



The list in the details pane provides the following information:

- **Name** - The name of the data encryption product or technology.
- **State** - Indicates whether integration is enabled for the given product or technology:
  - **Enabled** - “Encrypted” permissions can be applied.
  - **Disabled** - “Encrypted” permissions have no effect.
  - **Not Configured** - The setting is not defined in the DeviceLock Service settings file. This state is available in the [DeviceLock Service Settings Editor](#) and [DeviceLock Group Policy Manager](#).

To enable or disable integration, right-click in the list and then choose the **Enable** or **Disable** command. To set the state of Not Configured, use the **Undefine** command in the [DeviceLock Service Settings Editor](#) and [DeviceLock Group Policy Manager](#).

### **Data Encryption Products and Technologies**

As of this time DeviceLock provides integration with the following third-party products and technologies used for encrypting data on removable storage devices:

- [DriveCrypt](#)
- [Lexar JD SAFE S3000, Lexar JD SAFE S3000 FIPS](#)
- [Lexar SAFE PSD](#)
- [Rutoken Disk](#)
- [SafeDisk](#)
- [SafeGuard](#)
- [SafeToGo](#)
- [Symantec Drive Encryption \(formerly PGP Whole Disk Encryption\)](#)
- [TrueCrypt](#)
- [Windows BitLocker To Go](#)
- [Mac OS X FileVault](#)

---

### Note

DeviceLock does not ship with third-party encryption products and does not require them for its own functioning. The integration of DeviceLock with a third-party encryption product will only work when the third-party product is properly installed, configured, and functioning on the computer running DeviceLock Service.

---

If you do not want DeviceLock Service to apply “encrypted” permissions to devices encrypted by a particular product or technology listed above, disable integration by using the **Disable** command on the respective name in the details pane (see [Encryption](#)).

For more information on “encrypted” permissions, refer to the following sections of this manual:

[Permissions \(Regular Profile\)](#)

[“Encrypted” Rights Category](#)

### **DriveCrypt**

DeviceLock Service can detect DriveCrypt Plus Pack (DCPP) encrypted removable storage devices and apply “encrypted” permissions to them when the DriveCrypt Plus Pack product is installed on the computer running DeviceLock Service with integration enabled for DriveCrypt.

For details on DriveCrypt Plus Pack, refer to the Web site at [www.securstar.com/en/drivecrypt-plus-pack.html](http://www.securstar.com/en/drivecrypt-plus-pack.html).

### **Lexar JD SAFE S3000, Lexar JD SAFE S3000 FIPS**

DeviceLock Service can detect Lexar™ SAFE S3000 and/or SAFE S3000 FIPS USB flash drives and apply “encrypted” permissions to them if it has integration enabled for Lexar JD SAFE S3000 and/or Lexar JD SAFE S3000, respectively.

This product reached EOL. For details on Lexar SAFE S3000 and SAFE S3000 FIPS, refer to the “USB Flash Drive” section on Lexar’s Web site page at [www.lexar.com/faqs\\_cat/faqs-en-gb/](http://www.lexar.com/faqs_cat/faqs-en-gb/).

### **Lexar SAFE PSD**

DeviceLock Service can detect Lexar™ SAFE PSD S1100 USB flash drives and apply “encrypted” permissions to them if it has integration enabled for Lexar SAFE PSD.

### ***Rutoken Disk***

DeviceLock Service can detect Rutoken encrypted USB flash drives and apply “encrypted” permissions to them if it has integration enabled for Rutoken Disk.

For details on the Rutoken technology, see [www.rutoken.ru/products/all/rutoken-disk/](http://www.rutoken.ru/products/all/rutoken-disk/) (in Russian).

### ***SafeDisk***

DeviceLock Service can detect SafeDisk encrypted containers on USB flash drives and other removable media and apply “encrypted” permissions to them if it has integration enabled for SafeDisk.

For details on VIPNet Safe Disk, refer to the Web site at [infotecs.ru](http://infotecs.ru).

---

### **Note**

To access SafeDisk containers and work with their contents, users should have at least read access to unencrypted Removable devices.

---

### ***SafeGuard***

DeviceLock Service can detect Sophos SafeGuard Easy encrypted USB flash drives and other removable media and apply “encrypted” permissions to them if it has integration enabled for SafeGuard.

For details on Sophos SafeGuard Easy, refer to the Sophos Web site at [www.sophos.com/products/safeguard-encryption.aspx](http://www.sophos.com/products/safeguard-encryption.aspx).

### ***SafeToGo***

DeviceLock Service can detect SafeToGo™ encrypted USB flash drives and apply “encrypted” permissions to them if it has integration enabled for SafeToGo.

For details on SafeToGo™, refer to the Web site at [www.securedrives.com/products/safetogo-solo/](http://www.securedrives.com/products/safetogo-solo/).

### ***Symantec Drive Encryption (formerly PGP Whole Disk Encryption)***

DeviceLock Service can detect removable storage devices encrypted by Symantec Drive Encryption and apply “encrypted” permissions to them when the Symantec Drive Encryption product is installed on the computer running DeviceLock Service with integration enabled for Symantec Drive Encryption.

For details on Symantec Drive Encryption, refer to [www.broadcom.com/products/cyber-security/information-protection/encryption](http://www.broadcom.com/products/cyber-security/information-protection/encryption). For instructions on how to install and use PGP® Whole Disk Encryption with DeviceLock, see the [PGP/DeviceLock Integration Guide](#) created by PGP.

### ***TrueCrypt***

DeviceLock Service can detect removable storage devices encrypted by TrueCrypt and apply “encrypted” permissions to them when the TrueCrypt product is installed on the computer running DeviceLock Service with integration enabled for TrueCrypt.

This product reached the EOL, we recommend to use BitLocker instead.

---

**Note**

If the TrueCrypt volume type is “File-hosted (container)”, then, to access that container and work with its content, users should have at least read access to unencrypted Removable devices.

---

**Windows BitLocker To Go**

DeviceLock Service can detect BitLocker To Go encrypted drives and apply “encrypted” permissions to them if it has integration enabled for Windows BitLocker To Go.

For details on the BitLocker Drive Encryption technology included in Windows 7 and later versions of Windows, see Microsoft’s documentation at [docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731549\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731549(v=ws.10)) and [docs.microsoft.com/pl-pl/windows/security/information-protection/bitlocker/bitlocker-to-go-faq](https://docs.microsoft.com/pl-pl/windows/security/information-protection/bitlocker/bitlocker-to-go-faq).

---

**Note**

If integration with Windows BitLocker To Go is enabled, the “Deny write access to removable drives not protected by BitLocker” Group Policy setting cannot be enabled. (This setting is located in Computer Configuration\ Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives.)

---

**Mac OS X FileVault**

DeviceLock Service for Mac can detect FileVault encrypted external drives and apply “encrypted” permissions to them if it has integration enabled for Mac OS X FileVault. Integration with FileVault is not supported on the Windows operating system, so the Mac OS X FileVault item does not appear on the Encryption list in the details pane if the console is connected to a Windows-based computer.

For details on FileVault, refer to the Apple Web site at [support.apple.com/HT204837](https://support.apple.com/HT204837).

## Devices Node

The **Devices** node allows you to access the following functions of DeviceLock:

- Permissions for devices (see [Permissions \(Regular Profile\)](#), [Managing Offline Permissions for Devices](#))
- Auditing, shadowing and alerts for devices (see [Auditing, Shadowing & Alerts \(Regular Profile\)](#), [Managing Offline Audit, Shadowing and Alerts for Devices](#))
- Devices white list (see [USB Devices White List \(Regular Profile\)](#), [Managing Offline USB Devices White List](#))
- Media white list (see [Media White List \(Regular Profile\)](#), [Managing Offline Media White List](#))

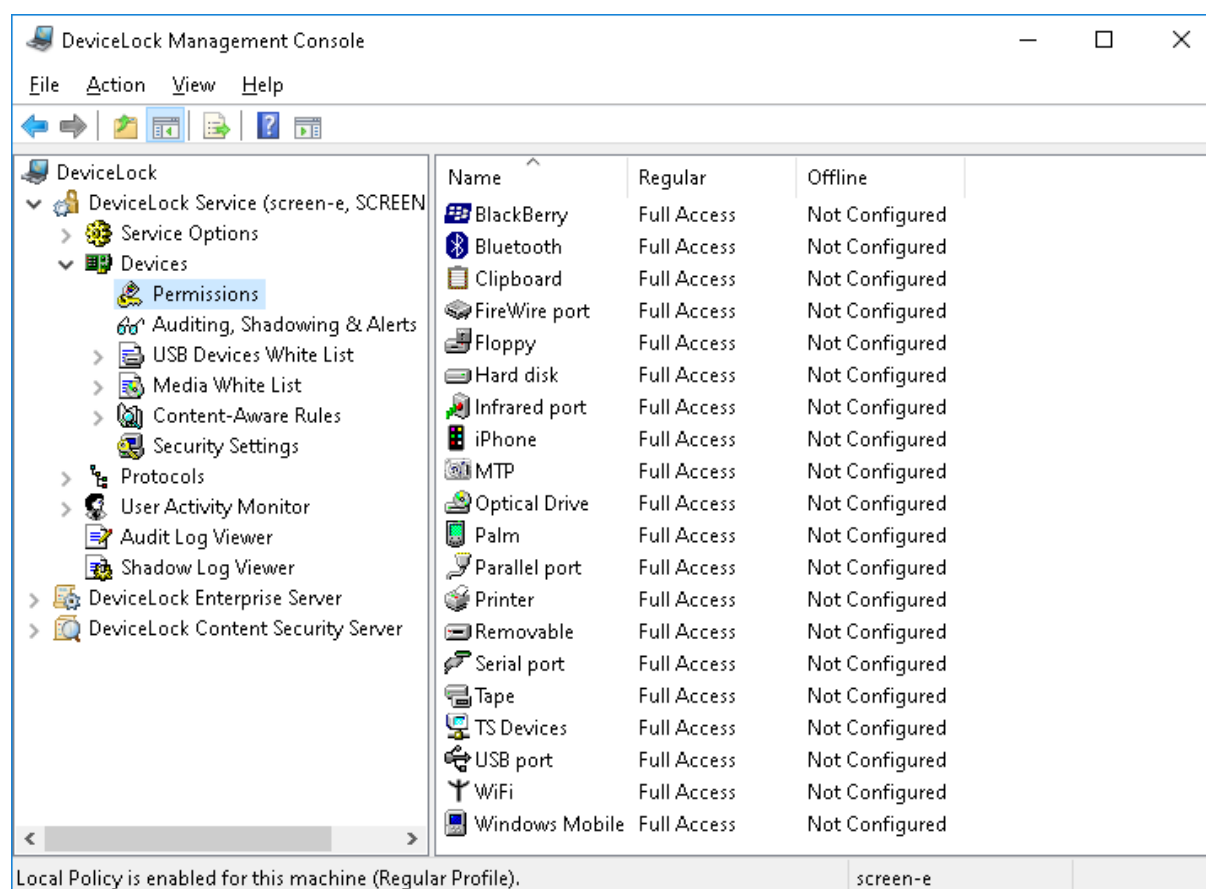
- Content-aware rules for devices (see [Rules for Devices](#), [Defining Rules for Devices](#), [Managing Offline Content-Aware Rules for Devices](#))
- Security settings for devices (see [Security Settings \(Regular Profile\)](#), [Managing Offline Security Settings for Devices](#))

The shortcut menu on this node provides the following command:

- **Undefine ContentLock Policy** - Resets parameters specific to ContentLock (all content-aware rules except those based on file types) to the unconfigured state.

## Permissions (Regular Profile)

The **Permissions** node lists the device types for which you can define user-level permissions.



### Note

When you set permissions for a device type, you set them for every device of that type. It is impossible to set different permissions for different devices if they are of the same type (such as removable drives). To define different permissions for USB devices even if they are of the same type, use the White List function (see [USB Devices White List \(Regular Profile\)](#)).

There are two levels of control: the interface (port) level and the type level. Some devices are checked at both levels, while others only at the one level - either interface (port) or type. For more

information on how access control works, refer to the [Managed Access Control](#) section of this manual.

DeviceLock supports the following types of devices:

- **BlackBerry** (type level) - Includes all BlackBerry devices with any type of the connection interface (USB, Bluetooth) to the computer.
- **Bluetooth** (type level) - Includes all internal and external Bluetooth devices with any type of the connection interface (USB, PCMCIA, etc.) to the computer.
- **Clipboard** - Includes the Windows Clipboard. DeviceLock controls copy/paste operations for data placed on the clipboard.

---

### Important

Right after the DeviceLock Service is installed, the user can copy and paste data between applications even if permissions are configured to deny access to the Clipboard. In this case, restart the computer for the Clipboard access settings to take effect.

---

- **FireWire port** (interface level) - Includes all devices that can be plugged into the FireWire (IEEE 1394) port, except the hub devices.
- **Floppy** (type level) - Includes all internal and external floppy drives with any connection interface (IDE, USB, PCMCIA, etc.). It is possible that some nonstandard floppy drives are recognized by Windows as removable devices, in this case DeviceLock treats such floppy drives as the **Removable** type as well.
- **Hard disk** (type level) - Includes all internal hard drives with any connection interface (IDE, SATA, SCSI, etc). DeviceLock treats all external USB, FireWire and PCMCIA hard drives as the Removable type. Also, DeviceLock treats as Removable some internal hard drives (usually SATA and SCSI) if they support the hot plug feature and Windows is not installed and running on them.

---

### Note

Even if you deny access to the Hard disk type, users with local administrator rights (the SYSTEM user and members of the local Administrators group) still can access the disk partition where Windows is installed and running.

---

- **Infrared port** (interface level) - Includes all devices that can be connected to the computer via the infrared (IrDA) port.
- **iPhone** (type level) - Includes all iPhone, iPod Touch, and iPad devices. DeviceLock controls iPhone, iPod Touch, and iPad devices that are working with a PC through the iTunes application or its API.
- **MTP** (type level) - Includes all devices (such as Android smartphones, etc.) that are working with a PC through the Media Transfer Protocol. DeviceLock controls devices with any type of connection interface (USB, IP, Bluetooth) to the computer.
- **Optical Drive** (type level) - Includes all internal and external CD/DVD/BD devices (readers and writers) with any connection interface (IDE, SATA, USB, FireWire, PCMCIA, etc).

- **Palm** (type level) - Includes all Palm OS devices with any type of connection interface (USB, COM, IrDA, Bluetooth, WiFi) to the computer. DeviceLock controls Palm OS devices that are working with a PC through the HotSync application.
- **Parallel port** (interface level) - Includes all devices that can be connected to the computer via the parallel (LPT) ports.
- **Printer** (type level) - Includes all local and network printers with any type of connection interface (USB, LPT, Bluetooth, etc) to the computer. DeviceLock can even optionally control virtual printers which do not send documents to real devices, but instead print to files (for example, PDF converters).
- **Removable** (type level) - Includes all internal and external devices with any connection interface (USB, FireWire, PCMCIA, IDE, SATA, SCSI, etc) that are recognized by Windows as removable devices (for example, USB flash drives, ZIP drives, card readers, magneto-optical drives, and so on). DeviceLock treats all external USB, FireWire and PCMCIA hard drives as the Removable type as well. Also, DeviceLock treats as Removable some internal hard drives (usually SATA and SCSI) if they support the hot plug feature and Windows is not installed and running on them.
- **Serial port** (interface level) - Includes all devices that can be connected to the computer via the serial (COM) ports, including internal modems.
- **Tape** (type level) - Includes all internal and external tape drives with any connection interface (SCSI, USB, IDE, etc).
- **TS Devices** (interface level) - Includes mapped drives (all hard, removable and optical drives), serial ports, USB devices and the clipboard redirected from remote terminals to virtual application or desktop sessions, as well as to virtual desktops that run in the server host environment. DeviceLock controls device, port and terminal clipboard redirections via Microsoft RDP, Citrix ICA, VMware PCoIP, HTML5/WebSockets remoting protocols in Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer and VMware View virtualization environments. In addition, for a guest Windows system that runs in VMware Workstation, VMware Player, Oracle VM VirtualBox or Windows Virtual PC virtualization solutions DeviceLock controls data copy operations between its Windows Clipboard and the clipboard of the host operating system.
- **USB port** (interface level) - Includes all devices that can be plugged into the USB port, except the hub devices.
- **WiFi** (type level) - Includes all internal and external WiFi devices with any type of connection interface (USB, PCMCIA, etc.) to the computer.

---

#### Note

Using the WiFi type you can control user access to the hardware device but not to the network.

---

- **Windows Mobile** (type level) - Includes all Windows Mobile devices with any type of connection interface (USB, COM, IrDA, Bluetooth, WiFi) to the computer. DeviceLock controls Windows Mobile devices that are working with a PC through the Windows Mobile Device Center (WMDC) or Microsoft ActiveSync application or its API.

## Setting Permissions

To set permissions for a device type, highlight it (use Ctrl and/or Shift to select several types simultaneously) and select **Set Permissions** or **Set Offline Permissions** from the shortcut menu available by a right mouse click. Alternatively, you can click the appropriate button on the toolbar.

---

### Note

You can define different online vs. offline permissions for the same user or sets of users. Online permissions (Regular Profile) apply to client computers that are working online. Offline permissions (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to set offline permissions, see [Managing Offline Permissions for Devices](#).

---

In [DeviceLock Group Policy Manager](#) or [DeviceLock Service Settings Editor](#), if you want to reset online (regular) permissions to the unconfigured state, select **Undefine** from the shortcut menu.

If you want to reset previously set offline permissions to the unconfigured state, select **Undefine Offline** from the shortcut menu. If offline permissions are undefined, regular permissions are applied to offline client computers.

In [DeviceLock Group Policy Manager](#) or [DeviceLock Service Settings Editor](#), if you want to block the inheritance of offline permissions and enforce regular permissions, select **Remove Offline** from the shortcut menu.

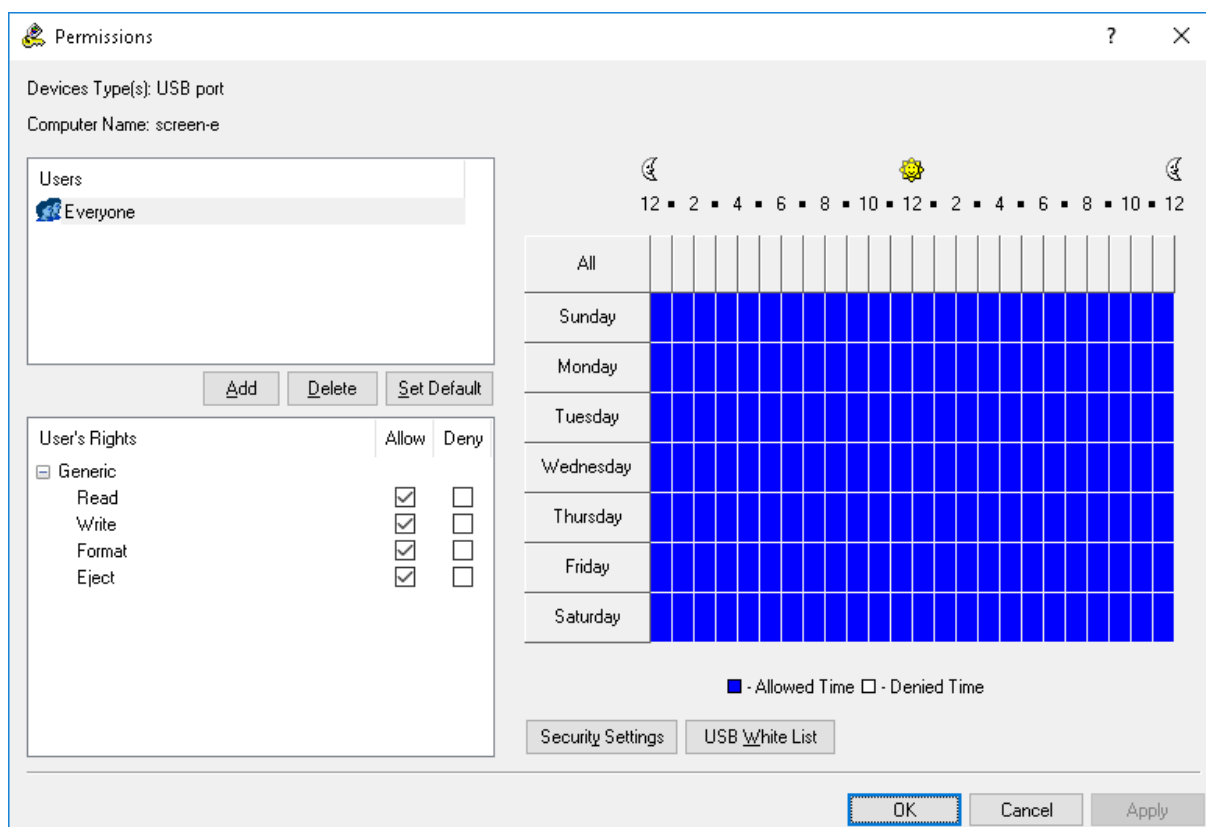
Online permissions for a device type can have one of the following states:

- **Configured** - Different accounts are assigned different permissions for the device type.
- **Full Access** - All accounts have full access to the device type.  
This state shows up, for example, when permissions are set only for the “Everyone” account so that it has full access to the device type.
- **No Access** - No accounts have access to the device type.  
This state shows up, for example, when the “Everyone” account is explicitly denied any access to the device type, or permissions are not set for any accounts. Note that the denial for the “Everyone” account overrides all permissions for other accounts.
- **Not Configured** - No permission settings are specified for the device type.

## Permissions Dialog Box

To set online (regular) permissions for a device type, highlight it (use Ctrl and/or Shift to select several types simultaneously) and select **Set Permissions** from the shortcut menu available by a right mouse click. Alternatively, you can click the appropriate button on the toolbar.





The names of the users and user groups assigned to a device type are shown in the list of accounts on the top left-hand side of the **Permissions** dialog box.

To add a new user or user group to the list of accounts, click **Add**. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using CTRL and/or SHIFT you can select and remove several records simultaneously.

Use the **Set Default** button to set default permissions for the device. For a list of permissions set by default, see [Default Permissions](#).

Using special time control, you can define a time when the selected user or user group will or will not have access to devices. Time control appears at the top-right side of the **Permissions** dialog box. Use the left mouse button and select the allowed time. To select a denied time use the right mouse button. Also, you can use the keyboard to set times - arrow keys for navigation and the spacebar to toggle allowed/denied time.

To specify the user actions to be allowed or denied, set the appropriate access rights. There are three categories of access rights:

- **Generic** - Rights that apply to most devices, except encrypted. For details, see ["Generic" Rights Category](#).
- **Encrypted** - Rights that apply to devices that DeviceLock recognizes as encrypted. For details, see ["Encrypted" Rights Category](#).

- **Special Permissions** - Rights that apply only to iPhone, Windows Mobile, Palm and Clipboard device types. For details, see [“Special Permissions” Rights Category](#).

If all **Allow** rights are enabled for the user account it means that this account has “full access” rights. If all **Deny** rights are enabled for the user account it means that this account has “no access” rights. If neither **Allow** nor **Deny** rights are enabled for the user account it means that this account inherits access rights from its user group (if there is no group to inherit rights from then this account has “no access” rights).

---

#### Note

The “no access” right has a priority over all other rights. It means that if the group to which some user belongs has the “no access” right but this user has “full access”, the user still cannot access a device. If you want to deny access for some user or group, you can just remove it from the account’s list, it is not necessary to add it with “no access”.

---

Also, the Everyone user has a priority over all other accounts. It means that if Everyone has the “no access” right, no one can access a device. The following message will appear: “You have denied everyone access to Device Type(s): <device type list>. No one will be able to access Device Type(s): <device type list>. Do you wish to continue?”

Even if you deny access to hard disks, users with local administrative privileges (the SYSTEM user and members of the local Administrators group) still can access the partition where Windows is installed and running.

We recommend that you add only those accounts (users and/or groups) to the list which should be able to access a device. If the account’s list is empty (contains no records at all) then no one can access a device. Also, it is recommended to add the SYSTEM user with “full access” to hard disks and optical drives.

On some systems, users may receive the following message when they log in: “Failed to configure a (n) CDROM Drive device. Check event log for details.” It means that the SYSTEM user cannot access DVD/CD/BD-ROM. To avoid this message, set the “full access” right for SYSTEM on Optical Drive.

### “Generic” Rights Category

“Generic” access rights apply to most device types. These rights do not affect access to devices that DeviceLock recognizes as encrypted (see [Encryption](#) for a list of such devices). The following rights are available in this category:

- **Read** - Enables data reading from the device. Applies to all device types except Clipboard and Printer.
- **Write** - Enables data writing to the device. With the exception of Windows Mobile, this right can be enabled for all devices only if **Read** is selected in the **Generic** group. It cannot be disabled for BlackBerry, Bluetooth, Infrared port, Parallel port, Serial port and WiFi device types. When **Write** is disabled for USB and FireWire ports it has the following effects: storage devices such as flash drives, floppies, hard disks, optical drives, etc. can be read, but not written to; non-storage devices such as printers, scanners, etc. cannot be accessed.

- **Format** - Enables the formatting, checking, and any other direct access of drives. This right can be enabled only if **Read** is selected in the **Generic** group. Applies only to FireWire port, Floppy, Hard disk, Removable and USB port device types. When this right is enabled for USB and FireWire ports, it affects only storage devices plugged into these ports.
- **Eject** - Enables ejection of the media. This right can be enabled only if **Read** is selected in the **Generic** group. This right controls only ejection via software. Hardware ejection using the eject button on a device's front panel cannot be prevented. Applies only to FireWire port, Floppy, Optical Drive, Removable and USB port device types. When this right is enabled for USB and FireWire ports it affects only storage devices plugged into these ports.
- **Execute** - Enables the remote code execution on the device side. Applies only to the Windows Mobile device type.
- **Modem** - Enables the use of the Internet Tethering feature. Applies only to the iPhone device type.
- **Print** - Enables document printing. Applies only to the Printer device type.
- **Copy to clipboard** - Enables data pasting from the clipboard. Applies only to the Clipboard device type. This right automatically grants full access to the clipboard.
- **Mapped Drives Read** - Enables data reading from mapped drives during a terminal session. Applies only to TS Devices.
- **Mapped Drives Write** - Enables data writing to mapped drives during a terminal session. Applies only to TS Devices.
- **Serial Port Access** - Enables access to serial ports during a terminal session. Applies only to TS Devices.
- **USB Devices Access** - Enables access to USB devices during a terminal session. Applies only to TS Devices.
- **Clipboard Incoming Text** - Enables pasting text data from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing Text** - Enables pasting text data from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Incoming Image** - Enables pasting graphical data from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing Image** - Enables pasting graphical data from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Incoming Audio** - Enables pasting audio data from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing Audio** - Enables pasting audio data from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Incoming File** - Enables pasting files from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing File** - Enables pasting files from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.

- **Clipboard Incoming Unidentified Content** - Enables pasting any other uncategorized content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing Unidentified Content** - Enables pasting any other uncategorized content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.

### “Encrypted” Rights Category

“Encrypted” access rights apply to [devices that DeviceLock recognizes as encrypted](#) (see also [Encryption](#) for further details). The following rights are available in this category:

- **Read** - Enables data reading from an encrypted device. Applies only to the Removable device type.
- **Write** - Enables data writing to an encrypted device. This right can be enabled only if **Read** is selected in the **Encrypted** group. Applies only to the Removable device type.
- **Format** - Enables the formatting, checking, and any other direct access of encrypted drives. This right can be enabled only if **Read** is selected in the **Encrypted** group. Applies only to the Removable device type.

### “Special Permissions” Rights Category

The rights in the “Special permissions” category apply only to iPhone, Windows Mobile, Palm and Clipboard device types. The content types (*Calendar, Contacts, Tasks*, etc.) controlled by these rights for iPhone, Windows Mobile, and Palm devices represent the same content types that exist in iTunes, HotSync, Microsoft ActiveSync and WMDC applications. For Palm devices, any **Write** right can be enabled only if the corresponding **Read** right is also enabled. The following rights are available in this category:

- **Read Calendar** - Enables reading the calendar on a mobile device from a PC.
- **Write Calendar** - Enables writing to a calendar on a mobile device from a PC.
- **Read Contact** - Enables reading contacts on a mobile device from a PC.
- **Write Contact** - Enables writing contacts from a PC to a mobile device.
- **Read E-mail** - Enables reading e-mails on a mobile device from a PC. For iPhone, this content type represents e-mail account settings but not messages because iTunes does not support sync of messages.
- **Write E-mail** - Enables writing e-mails from a PC to a mobile device. For iPhone, this content type represents e-mail account settings but not messages because iTunes does not support sync of messages.
- **Read Attachment** - Enables reading e-mail attachments on a Windows Mobile device from a PC. This right can be enabled only if **Read E-mail** is selected in the **Special Permissions** group.
- **Write Attachment** - Enables writing e-mail attachments from a PC to a Windows Mobile device. This right can be enabled only if **Write Email** is selected in the **Special Permissions** group.
- **Read Favorite** - Enables reading favorites on a Windows Mobile device and iPhone from a PC.
- **Write Favorite** - Enables writing favorites from a PC to a Windows Mobile device and iPhone.

- **Read File** - Enables reading files on a mobile device from a PC. For iPhone, data flows of the *Applications* iTunes type are treated as files.
- **Write File** - Enables writing files from a PC to a mobile device. For a Palm device this right also enables **Write Document** in the **Special Permissions** group. For iPhone, data flows of the *Applications* iTunes type are treated as files.
- **Read Media** - Enables reading media content using Windows Media Player on a Windows Mobile device and reading media files on a Palm device and iPhone from a PC. This right can be enabled only if **Read Files** is selected in the **Special Permissions** group. For a Windows Mobile device, this option also requires selecting **Execute** from the **Generic** group. For iPhone, the media content type consists of the following iTunes types: *Ringtones, Music, Audiobooks, Photos, Podcasts* (Audio & Video), *Movies, TV shows, Rented Movies*.
- **Write Media** - Enables writing media content using Windows Media Player to a Windows Mobile device and writing media files to a Palm device and iPhone from a PC. This right can be enabled only if **Write Files** is selected in the **Special Permissions** group and, for a Windows Mobile device, if **Execute** is selected from the **Generic** group. For iPhone, the media content type consists of the following iTunes types: *Ringtones, Music, Audiobooks, Photos, Podcasts* (Audio & Video), *Movies, TV shows, Rented Movies*.
- **Read Backup** - Enables creating the iPhone backup by reading the device data from a PC.

---

#### Note

An iPhone device is backed up by iTunes each time users sync with iTunes (automatically on the first sync, every time they connect it to the computer). To allow synchronization to complete successfully, grant the **Read Backup** permission to users for the iPhone device type. Otherwise, if iTunes automatically creates an iPhone backup, the synchronization session will be interrupted. To avoid interrupting the synchronization process, users should set iTunes to sync only the content to which they are allowed access.

---

- **Write Backup** - Enables restoring iPhone by writing the device backup data from a PC.
- **Read Note** - Enables reading notes on a mobile device from a PC. For a Palm device this right controls *Memos* and *Note Pad* content types.
- **Write Note** - Enables writing notes from a PC to a mobile device. For a Palm device this right controls *Memos* and *Note Pad* content types.
- **Read Pocket Access** - Enables reading Pocket Access databases on a Windows Mobile device from a PC.
- **Write Pocket Access** - Enables writing Pocket Access databases from a PC to a Windows Mobile device.
- **Read Task** - Enables reading tasks on a mobile device from a PC.
- **Write Task** - Enables writing tasks from a PC to a mobile device.
- **Read Expense** - Enables reading Palm Expense application data on a Palm device from a PC.
- **Write Expense** - Enables writing Palm Expense application data from a PC to a Palm device.
- **Read Document** - Enables reading Palm documents on a Palm device from a PC. This right can be enabled only if **Read Files** is selected in the **Special Permissions** group.

- **Write Document** - Enables writing Palm documents from a PC to a Palm device. This right can be enabled only if **Write Files** is selected in the **Special Permissions** group.
- **Read Unidentified Content** - Enables reading any other uncategorized content type on a Windows Mobile device from a PC.
- **Write Unidentified Content** - Enables writing any other uncategorized content type from a PC to a Windows Mobile device.
- **Copy Text** - Enables pasting text data from the clipboard.
- **Copy Image** - Enables pasting graphical data from the clipboard.
- **Copy Audio** - Enables pasting audio data from the clipboard.
- **Copy File** - Enables pasting files from the clipboard.
- **Copy Unidentified Content** - Enables pasting any other uncategorized content type from the clipboard.
- **Screenshot** - Enables capturing screenshots of the entire screen, the active window or any segment of the screen.

---

#### Note

Screenshots made with special programs for creating screenshots are saved directly to files, while screenshots taken with the PRINT SCREEN key are first copied to the clipboard and then pasted into the desired program (for example, Microsoft Word or Paint). When using special programs, the screenshot event falls into the audit immediately when a screenshot is created with such a program, whereas when the PRINT SCREEN key is pressed, the event falls into the audit only when the screenshot is pasted into the desired program.

To capture screenshots by pressing the PRINT SCREEN key, the user must have the **Screenshot** and **Copy Image** rights. If users do not have the **Screenshot** right, they cannot take screenshots with either the PRINT SCREEN key, or using special programs for creating screenshots.

---

When using special permissions, consider the following:

- The **Copy Text**, **Copy Image**, **Copy Audio**, **Copy File**, and **Copy Unidentified Content** rights do not control data copying to the clipboard. Users can always copy data to the clipboard regardless of the rights they have.
- In some cases, users can use the clipboard to move different types of data in Rich Text Format (RTF), such as Text, Image, File, either individually or in different combinations. To allow users to copy and paste different types of RTF data, you must grant them the appropriate rights (such as **Copy Text**, **Copy Image** and **Copy File**).
- If access (read and/or write) to some content type is denied during the iPhone or Windows Mobile synchronization process, you have to replug the device in order to continue using the iPhone or Windows Mobile device.
- When users attempt to synchronize a Palm handheld device over a network and DeviceLock denies access to some content type, the synchronization session is interrupted. To avoid this situation, users should set the HotSync application to sync only the content to which they are allowed access before attempting synchronization.

## Default Permissions

The **Permissions** dialog box provides the option to set default permissions to access devices. These permissions are assigned to the Administrators and Everyone groups, and to the SYSTEM account. The following table lists the default permissions for each type of device.

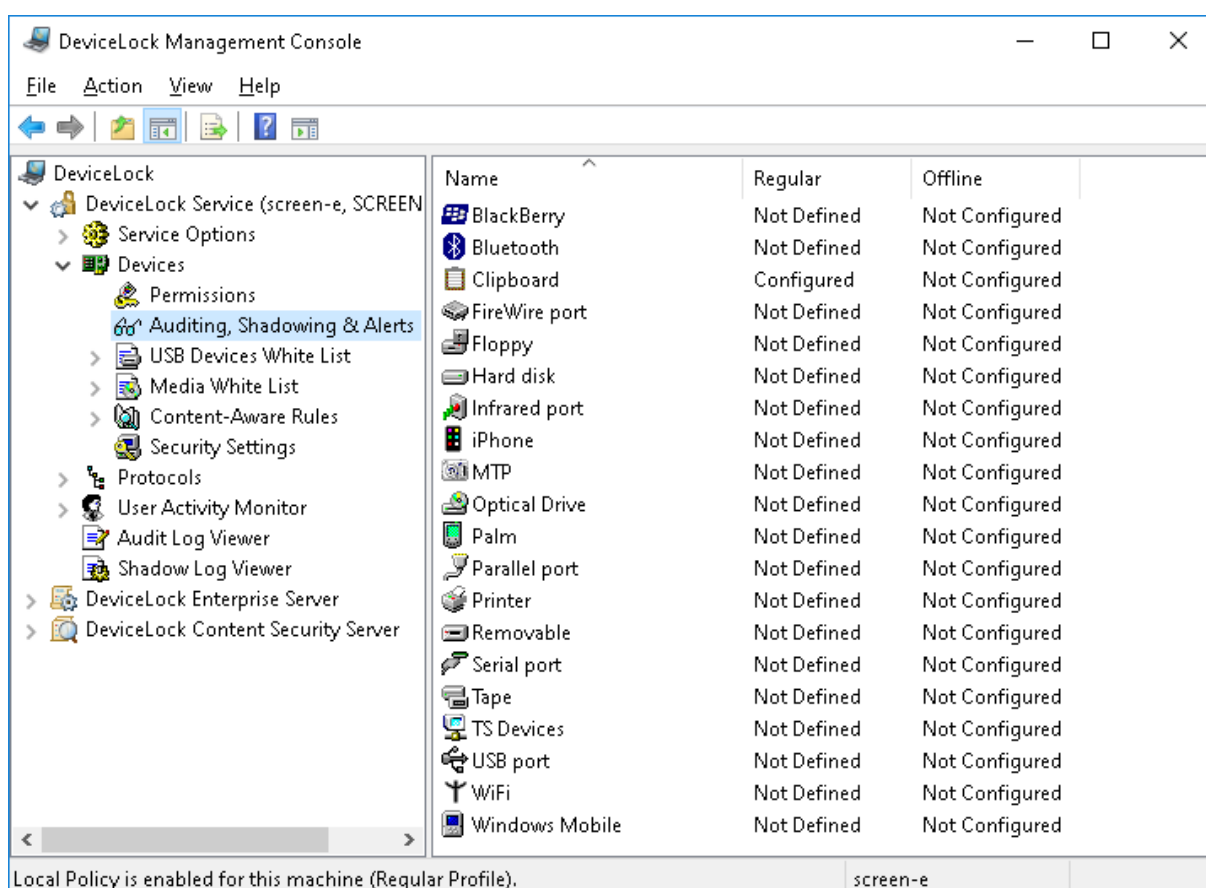
Account/ Device type	Everyone	Administrators	SYSTEM
BlackBerry	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Bluetooth	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Clipboard	Generic: Copy to clipboard  Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content	Generic: Copy to clipboard  Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content	Generic: Copy to clipboard  Special Permissions: Copy Text, Copy Image, Copy Audio, Copy File, Screenshot, Copy Unidentified Content
FireWire port	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
Floppy	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
Hard disk	Generic: Read, Write	Generic: Read, Write, Format	Generic: Read, Write, Format
Infrared port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
iPhone	Generic: Read, Write, Modem	Generic: Read, Write, Modem	Generic: Read, Write, Modem
MTP	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Optical Drive	Generic: Read, Write, Eject	Generic: Read, Write, Eject	Generic: Read, Write, Eject
Palm	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Parallel port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write

Printer	Generic: Print	Generic: Print	Generic: Print
Removable	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
	Encrypted: Read, Write, Format	Encrypted: Read, Write, Format	Encrypted: Read, Write, Format
Serial port	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Tape	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
TS Devices	Generic: Mapped Drives Read, Serial Port Access, USB Devices Access, Clipboard Incoming Text, Clipboard Incoming Image, Clipboard Incoming Audio, Clipboard Incoming File, Clipboard Incoming Unidentified Content	Generic: Mapped Drives Read, Mapped Drives Write, Serial Port Access, USB Devices Access, Clipboard Incoming Text, Clipboard Outgoing Text, Clipboard Incoming Image, Clipboard Outgoing Image, Clipboard Incoming Audio, Clipboard Outgoing Audio, Clipboard Incoming File, Clipboard Outgoing File, Clipboard Incoming Unidentified Content, Clipboard Outgoing Unidentified Content	Generic: Mapped Drives Read, Mapped Drives Write, Serial Port Access, USB Devices Access, Clipboard Incoming Text, Clipboard Outgoing Text, Clipboard Incoming Image, Clipboard Outgoing Image, Clipboard Incoming Audio, Clipboard Outgoing Audio, Clipboard Incoming File, Clipboard Outgoing File, Clipboard Incoming Unidentified Content, Clipboard Outgoing Unidentified Content
USB port	Generic: Read, Write, Eject	Generic: Read, Write, Format, Eject	Generic: Read, Write, Format, Eject
WiFi	Generic: Read, Write	Generic: Read, Write	Generic: Read, Write
Windows Mobile	Generic: Read, Write, Execute	Generic: Read, Write, Execute	Generic: Read, Write, Execute

## Auditing, Shadowing & Alerts (Regular Profile)

The **Auditing, Shadowing & Alerts** node lists the device types for which you can define user-level audit, shadowing rules and alerts.





There is not much difference between setting up permissions and defining audit, shadowing rules and alerts so you should first read the [Permissions \(Regular Profile\)](#) section of this manual.

DeviceLock Service can use the standard Windows event logging subsystem to log a device's information. It is extremely useful for system administrators because they can use any event log reading software to view the DeviceLock audit log. You can use the standard Event Viewer, for example. Also, DeviceLock Service can use its own protected proprietary log. The data from this log is sent to DeviceLock Enterprise Server and stored centrally in the database. One more option is to store data on a syslog server. The data storage options are determined by the [Audit log type](#) parameter in [Service Options](#).

DeviceLock Management Console has its own built-in audit log viewer that represents information from the event log in a more convenient form. For more information, see [Audit Log Viewer \(Service\)](#).

To view the audit log stored on DeviceLock Enterprise Server, use the server's audit log viewer (see [Audit Log Viewer \(Server\)](#)).

Also there is an extended audit's feature called data shadowing - the ability to mirror all data copied to external storage devices or transferred through serial and parallel ports. A full copy of the data is logged. The shadow log is stored locally in the folder specified by the [Local storage directory](#) parameter and it can be transferred to DeviceLock Enterprise Server specified by the [DeviceLock Enterprise Server\(s\)](#) parameter, to be stored in DeviceLock Enterprise Server's database on SQL Server.

To view the locally stored shadow log, use DeviceLock Management Console's built-in shadow log viewer. For more information, see [Shadow Log Viewer \(Service\)](#).

To view the shadow log stored on DeviceLock Enterprise Server, use the server's shadow log viewer (see [Shadow Log Viewer \(Service\)](#)).

## Defining Audit and Shadowing Rules

To define audit and shadowing rules for a device type, highlight it (use Ctrl and/or Shift to select several types simultaneously) and select **Set Auditing, Shadowing & Alerts** or **Set Offline Auditing, Shadowing & Alerts** from the shortcut menu available by a right mouse click. Alternatively, you can click the appropriate button on the toolbar.

---

### Note

You can define different online vs. offline audit and shadowing rules for the same user or sets of users. Online audit and shadowing rules (Regular Profile) apply to client computers that are working online. Offline audit and shadowing rules (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define offline audit and shadowing rules, see [Managing Offline Audit, Shadowing and Alerts for Devices](#).

---

In [DeviceLock Group Policy Manager](#) or [DeviceLock Service Settings Editor](#), if you want to reset online (regular) audit and shadowing rules to the unconfigured state, select **Undefine** from the shortcut menu.

If you want to return previously defined offline audit and shadowing rules to the unconfigured state, select **Undefine Offline** from the shortcut menu. If offline rules are undefined, regular rules are applied to offline client computers.

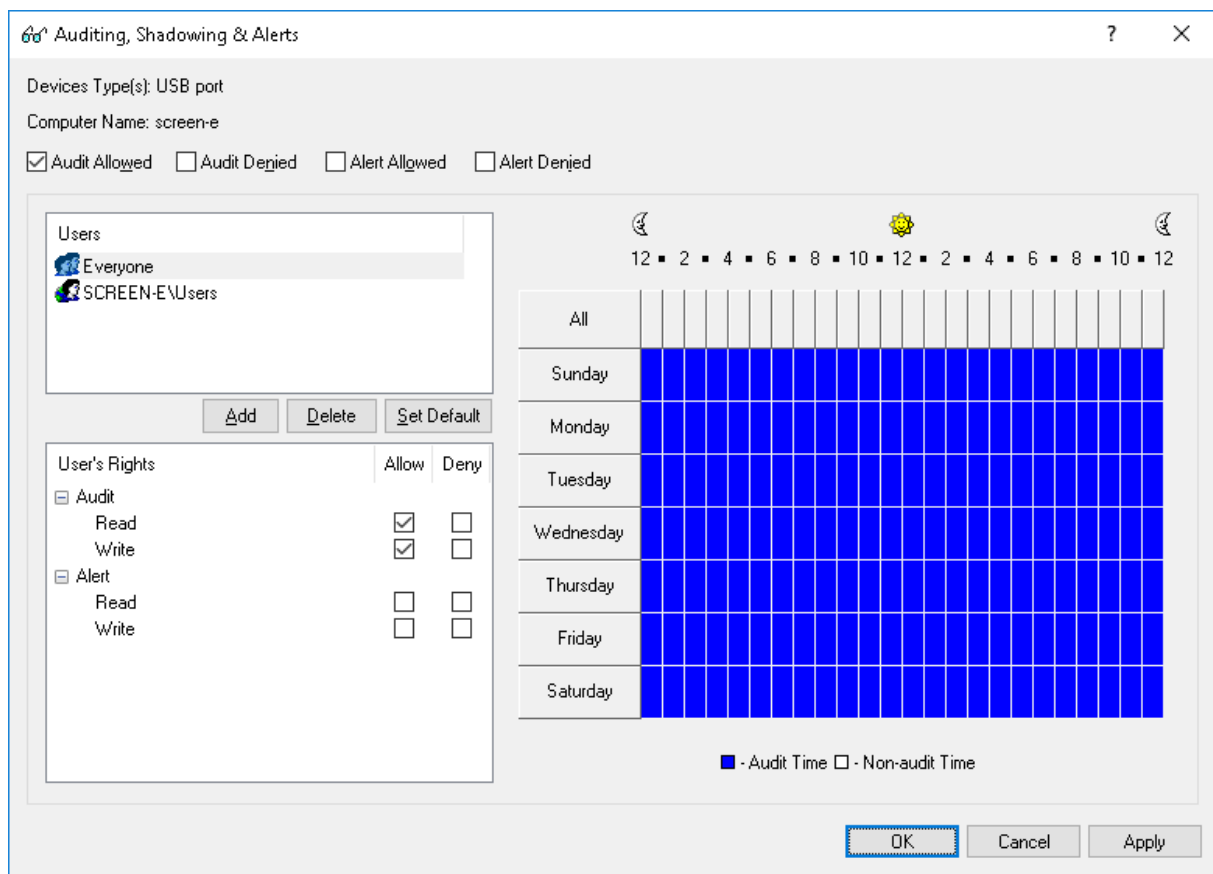
In [DeviceLock Group Policy Manager](#) or [DeviceLock Service Settings Editor](#), if you want to block the inheritance of offline audit and shadowing rules and enforce regular audit and shadowing rules, select **Remove Offline** from the shortcut menu.

Online audit, shadowing rules and alerts for a device type can have one of the following states:

- **Not Defined** - Audit, shadowing rules, and alerts are not defined for the device type.
- **Configured** - Audit, shadowing rules and/or alerts are defined for the device type.
- **No Audit** - Settings for the device type do not allow audit, shadowing, and alerts for any accounts.

## Auditing, Shadowing & Alerts Dialog Box

To define online (regular) audit and shadowing rules for a device type, highlight it (use Ctrl and/or Shift to select several types simultaneously) and select **Set Auditing, Shadowing & Alerts** from the shortcut menu available by the right mouse click. Alternatively, you can click the appropriate button on the toolbar.



There are two types of user access that can be logged to the audit log:

- **Allowed**- All access attempts that were permitted by DeviceLock Service, that is, the user was able to access a device.
- **Denied** - All access attempts that were blocked by DeviceLock Service, that is, the user was not able to access a device.

To enable logging to the audit log for one or both of these access types, check **Audit Allowed** and/or **Audit Denied**. These flags are not linked to users/groups, they are related to a whole device type.

The names of the users and user groups assigned to a device type are shown in the list of accounts on the top left-hand side of the **Auditing, Shadowing & Alerts** dialog box.

To add a new user or user group to the list of accounts, click **Add**. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using CTRL and/or SHIFT you can select and remove several records simultaneously.

Use the **Set Default** button to set default audit and shadowing rules for devices: members of the Users group and the Everyone account have **Read** and **Write** audit rights and shadowing is disabled for them.

Using special time control, you can define a time when the audit rule for the selected user or user group will or will not be active. Time control appears at the top-right side of the **Auditing, Shadowing & Alerts** dialog box. Use the left mouse button and select the time when the rule is active (audit time). To select a time when the rule is not active (non-audit time), use the right mouse button. Also, you can use the keyboard to set times - arrow keys for navigation and the spacebar to toggle audit/non-audit time.

To specify the user actions subject to logging, set the appropriate rights. There are two categories of rights:

- **Audit** - Rights that govern the logging of user actions to the Audit log. For details, see [“Audit” Rights Category](#).
- **Shadowing** - Rights that govern the logging of user actions to the Shadow log. For details, see [“Shadowing” Rights Category](#).

---

#### Note

If data transmission is blocked by permissions, a shadow copy of this data is not created. In this case DeviceLock blocks the transmission of data before it is captured. Exception: If data is being inspected by Content-Aware Rules, then DeviceLock creates the shadow copy even if permissions block the transmission of that data.

---

#### Recommendations

Audit records may not be logged despite the existing audit rules. This issue is usually caused by the **Audit Allowed** and **Audit Denied** check boxes not selected in the audit rules settings. The existing logging configuration in this case is not correct, which leads to the absence of audit log records.

When configuring audit rules, make sure that at least one of the **Audit Allowed** and **Audit Denied** check boxes is selected.

Also note that audit events are not logged at the USB interface level for whitelisted devices (see [USB Devices White List \(Regular Profile\)](#)), as well as for devices excluded from access control by security settings (see [Security Settings \(Regular Profile\)](#)).

#### “Audit” Rights Category

“Audit” rights are intended to specify what actions must be logged in the Audit log. The following rights are available in this category:

- **Read** - Log the read access attempts. For BlackBerry, Bluetooth, FireWire port, Infrared port, Parallel port, Serial port, USB port and WiFi device types, this right can be enabled only if **Write** is selected in the **Audit** group.
- **Write** - Log the write access attempts. For BlackBerry, Bluetooth, FireWire port, Infrared port, Parallel port, Serial port, USB port and WiFi device types, this right can be enabled only if **Read** is selected in the **Audit** group.
- **Format** - Log the direct write access attempts (e.g. formatting). Applies only to Floppy, Hard disk and Removable device types.

- **Print** - Log all attempts to send documents to printers. Applies only to the Printer device type.
- **Execute** - Log access attempts to remotely execute a code on the device's side. Applies only to the Windows Mobile device type.
- **Read Non-files** - Log the read access attempts for non-file objects (*Calendar, Contacts, Tasks*, etc.). Applies only to iPhone, Windows Mobile and Palm device types.
- **Write Non-files** - Log the write access attempts for non-file objects (*Calendar, Contacts, Tasks*, etc.). Applies only to iPhone, Windows Mobile and Palm device types.
- **Copy** - Log all attempts to paste data from the clipboard and capture screen shots. Applies only to Clipboard.
- **Mapped Drives Read** - Log all attempts to read data from mapped drives during a terminal session. Applies only to TS Devices.
- **Mapped Drives Write** - Log all attempts to write data to mapped drives during a terminal session. Applies only to TS Devices.
- **Serial Port Access** - Log all attempts to access serial ports during a terminal session. Applies only to TS Devices.
- **USB Devices Access** - Log all attempts to access USB devices during a terminal session. Applies only to TS Devices.
- **Clipboard Incoming** - Log all attempts to paste clipboard data (text data, graphical data, audio data, files and any other unidentified data) to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing** - Log all attempts to paste clipboard data (text data, graphical data, audio data, files and any other unidentified data) from a terminal session/virtual machine. Applies only to TS Devices.

For details on audit-related rights specific to each type of device, see [Summary of Audit and Shadowing Rights by Device Type](#).

### “Shadowing” Rights Category

“Shadowing” rights are intended to specify what actions must be logged in the Shadow log. The rights in this category are as follows:

- **Read** - Enables shadowing of all data read by the user. Applies only to MTP.
- **Write** - Enables shadowing of all data written by the user. Applies only to Floppy, iPhone, MTP, Optical Drive, Parallel port, Removable, Serial port, Windows Mobile and Palm devices.
- **Format** - Enables shadowing of raw data written by the user via the direct disk access (such as formatting). Applies only to Floppy and Removable device types.
- **Print** - Enables shadowing of all documents sent to printers. These documents will be available for viewing (see the [Open](#) command description in the [Shadow Log Viewer \(Service\)](#) section). Applies only to the Printer device type.
- **Write Non-files** - Enables shadowing of all non-file objects (*Calendar, Contacts, Tasks*, etc.) written by the user. Applies only to iPhone, Windows Mobile and Palm device types.

- **Mapped Drives Write** - Enables shadowing of all data written by the user. Applies only to TS Devices.
- **Copy** - Enables shadowing of pasted clipboard data and captured screen shots. Applies only to Clipboard.
- **Clipboard Incoming** - Enables shadowing of clipboard data pasted to a terminal session/virtual machine. Applies only to TS Devices.
- **Clipboard Outgoing** - Enables shadowing of clipboard data pasted from a terminal session/virtual machine. Applies only to TS Devices.

For a details on shadowing-related rights specific to each type of device, see [Summary of Audit and Shadowing Rights by Device Type](#).

## Summary of Audit and Shadowing Rights by Device Type

This section provides a list of audit and shadow copy rights for each type of device, and describes the information recorded in the relevant logs. For each event, DeviceLock Service logs the type of the event, the date and time that the event occurred, the type of the device where the event occurred, the reason (cause) of the event, the user name and process that caused the event. Besides, additional information about events is logged that depends upon the type of device:

- [BlackBerry](#)
- [Bluetooth](#)
- [Clipboard](#)
- [FireWire port](#)
- [Floppy](#)
- [Hard disk](#)
- [Infrared port](#)
- [iPhone](#)
- [MTP](#)
- [Optical Drive](#)
- [Palm](#)
- [Parallel port](#)
- [Printer](#)
- [Removable](#)
- [Serial port](#)
- [Tape](#)
- [TS Devices](#)
- [USB port](#)
- [WiFi](#)
- [Windows Mobile](#)

### BlackBerry

Rights applicable to the BlackBerry device type:

- Audit: Read  
*Device Access action is written to the audit log.*
- Audit: Write/Print  
*Device Access action is written to the audit log.*

## Bluetooth

Rights applicable to the Bluetooth device type:

- Audit: Read  
*Device Access action is written to the audit log.*
- Audit: Write/Print  
*Device Access action is written to the audit log.*

## Clipboard

Rights applicable to the Clipboard device type:

- Audit: Copy  
*Copy Text, Copy File, Copy Image, Copy Audio, Copy RTF (Image), Copy RTF (File), Copy RTF (Text, Image), Copy RTF (Text, File), Copy RTF (Image, File), Copy RTF (Text, Image, File), Copy Unidentified, Screenshot actions, file names, process name and PID are written to the audit log.*
- Shadowing: Copy  
*All data placed on the clipboard are written to the shadow log.*

## FireWire port

Rights applicable to the FireWire port device type:

- Audit: Read  
*Insert, Remove and Device Access actions, device names and Device ID are written to the audit log.*
- Audit: Write/Print  
*Insert, Remove and Device Access actions, device names and Device ID are written to the audit log.*

## Floppy

Rights applicable to the Floppy device type:

- Audit: Read  
*Read, Mount and Unmount actions and file names are written to the audit log.*
- Audit: Write/Print  
*Delete, Write, Restore and Rename actions and file names are written to the audit log.*
- Audit: Format  
*Format action and disk name are written to the audit log.*
- Shadowing: Write/Print  
*Files are written to the shadow log.*
- Shadowing: Format  
*Raw data is written to the shadow log.*

## Hard disk

Rights applicable to the Hard disk device type:

- Audit: Read  
*Read action and file names are written to the audit log.*
- Audit: Write/Print  
*Write, Rename and Delete actions and file names are written to the audit log.*
- Audit: Format  
*Format action and disk name are written to the audit log.*

## Infrared port

Rights applicable to the Infrared port device type:

- Audit: Read  
*Device Access action is written to the audit log.*
- Audit: Write/Print  
*Device Access action is written to the audit log.*

## iPhone

Rights applicable to the iPhone device type:

- Audit: Read  
*Read File action and file names are written to the audit log.*
- Audit: Write/Print  
*Write File, Rename File and Delete File actions and file names are written to the audit log.*
- Audit: Read Non-files  
*Read Calendar, Read Contact, Read Favorite, Read E-mail, Read Backup, Read Note and Read Media actions and object names are written to the audit log.*
- Audit: Write Non-files  
*Write Calendar, Delete Calendar, Write Contact, Delete Contact, Write Favorite, Delete Favorite, Write E-mail, Delete E-mail, Write Backup, Write Note, Delete Note, Write Media, Rename Media and Delete Media actions and object names are written to the audit log.*
- Shadowing: Write/Print  
*Files are written to the shadow log.*
- Shadowing: Write Non-files  
*All data that contains non-file objects (Calendar, Contacts, etc.) is written to the shadow log.*

## MTP

Rights applicable to the MTP device type:

- Audit: Read  
*Read action and file names are written to the audit log.*



- Audit: Write/Print  
*Delete, Rename and Write actions and file names are written to the audit log.*
- Shadowing: Read  
*Files are written to the shadow log.*
- Shadowing: Write/Print  
*Files are written to the shadow log.*

## Optical Drive

Rights applicable to the Optical Drive device type:

- Audit: Read  
*Read and Eject actions and file names are written to the audit log.*
- Audit: Write/Print  
*Write and Format actions and file names are written to the audit log.*
- Shadowing: Write/Print  
*CD/DVD/BD images in the CUE format and/or files are written to the shadow log.*

## Palm

Rights applicable to the Palm device type:

- Audit: Read  
*Read File action, file names and the Sync flag are written to the audit log.*
- Audit: Write/Print  
*Write File action, file names and the Sync flag are written to the audit log.*
- Audit: Read Non-files  
*Read Calendar, Read Contact, Read Expense, Read E-mail, Read Document, Read Memo, Read Notepad, Read Task and Read Media actions and object names are written to the audit log.*
- Audit: Write Non-files  
*Write Calendar, Write Contact, Write Expense, Write E-mail, Write Document, Write Memo, Write Notepad, Write Task, Write Media and Install actions and object names are written to the audit log.*
- Shadowing: Write/Print  
*Files are written to the shadow log.*
- Shadowing: Write Non-files  
*All data that contains non-file objects (Calendar, Contacts, Tasks, etc.) is written to the shadow log.*

## Parallel port

Rights applicable to the Parallel port device type:

- Audit: Read  
*Device Access action is written to the audit log.*
- Audit: Write/Print  
*Device Access action is written to the audit log.*
- Shadowing: Write/Print  
*All data sent to the port is written to the shadow log.*

## Printer

Rights applicable to the Printer device type:

- Audit: Write/Print  
*Print action, documents and printer names are written to the audit log.*
- Shadowing: Write/Print  
*All data sent to the printer is written to the shadow log in the PDF format.*

## Removable

Rights applicable to the Removable device type:

- Audit: Read  
*Read, Read Encrypted, Eject, Mount and Unmount actions and file names are written to the audit log.*
- Audit: Write/Print  
*Delete, Delete Encrypted, Rename, Rename Encrypted, Write, Write Encrypted, Restore and Restore Encrypted actions and file names are written to the audit log.*
- Audit: Format  
*Format, Format Encrypted actions and disk name are written to the audit log.*
- Shadowing: Write/Print  
*Files are written to the shadow log.*
- Shadowing: Format  
*Raw data is written to the shadow log.*

## Serial port

Rights applicable to the Serial port device type:

- Audit: Read  
*Device Access action is written to the audit log.*
- Audit: Write/Print  
*Device Access action is written to the audit log.*
- Shadowing: Write/Print  
*All data sent to the port is written to the shadow log.*

## Tape

Rights applicable to the Tape device type:

- Audit: Read  
*Read, Eject actions and device names is written to the audit log.*
- Audit: Write/Print  
*Write action and device names are written to the audit log.*

## TS Devices

Rights applicable to the TS Devices device type:

- Audit: Mapped Drives Read  
*Read action, drive name and path to the file are written to the audit log.*
- Audit: Mapped Drives Write  
*Write action, drive name and path to the file are written to the audit log.*
- Audit: Serial Port Access  
*Device Access action and name of the serial port are written to the audit log.*
- Audit: USB Devices Access  
*Device Access action and device name are written to the audit log.*
- Audit: Clipboard Incoming  
*Incoming Text, Incoming Image, Incoming Audio, Incoming File, Incoming RTF (Image), Incoming RTF (File), Incoming RTF (Text, Image), Incoming RTF (Text, File), Incoming RTF (Image, File), Incoming RTF (Text, Image, File), Incoming Unidentified actions, the file name or data object name, process name and PID are written to the audit log.*
- Audit: Clipboard Outgoing  
*Outgoing Text, Outgoing Image, Outgoing Audio, Outgoing File, Outgoing RTF (Image), Outgoing RTF (File), Outgoing RTF (Text, Image), Outgoing RTF (Text, File), Outgoing RTF (Image, File), Outgoing RTF (Text, Image, File), Outgoing Unidentified actions, the file name or data object name, process name and PID are written to the audit log.*
- Shadowing: Mapped Drives Write  
*Files are written to the shadow log.*
- Shadowing: Clipboard Incoming  
*All data pasted from the clipboard are written to the shadow log.*
- Shadowing: Clipboard Outgoing  
*All data placed on the clipboard are written to the shadow log.*

## USB port

Rights applicable to the USB port device type:

- Audit: Read  
*Insert, Remove and Device Access actions, device names and Device ID are written to the audit log.*
- Audit: Write/Print  
*Insert, Remove and Device Access actions, device names and Device ID are written to the audit log.*

## WiFi

Rights applicable to the WiFi device type:

- Audit: Read  
*Device Access action is written to the audit log.*
- Audit: Write/Print  
*Device Access action is written to the audit log.*

## Windows Mobile

Rights applicable to the Windows Mobile device type:

- **Audit: Read**  
*Read File action, file names and flag (Sync) are written to the audit log.*
- **Audit: Write/Print**  
*Write File, Delete File, Rename, Overwrite and Create Shortcut actions, file names and flags are written to the audit log.*
- **Audit: Execute**  
*Invoke and Execute actions, file names and function (procedure) names are written to the audit log.*
- **Audit: Read Non-files**  
*Read Calendar, Read Contact, Read Favorite, Read E-mail, Read Attachment, Read Note, Read Task, Read Media, Read Pocket Access and Read Unidentified actions and object names are written to the audit log.*
- **Audit: Write Non-files**  
*Write Calendar, Delete Calendar, Write Contact, Delete Contact, Write Favorite, Delete Favorite, Write E-mail, Delete E-Mail, Write Attachment, Delete Attachment, Write Note, Delete Note, Write Task, Delete Task, Write Media, Delete Media, Write Pocket Access, Delete Pocket Access, Write Unidentified and Delete Unidentified actions and object names are written to the audit log.*
- **Shadowing: Write/Print**  
*Files are written to the shadow log.*
- **Shadowing: Write Non-files**  
*All data that contains non-file objects (Calendar, Contacts, Tasks, etc.) is written to the shadow log.*

## Enabling Alerts

In the [Auditing, Shadowing & Alerts Dialog Box](#), you can enable alerts that are sent when a specific user attempts to access a specific device type.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for specific events, you must configure alert settings in **Service Options** (see [Alerts](#)).

Alerts for specific access-related events are enabled in the **Auditing, Shadowing & Alerts** dialog box. Enabling alerts is similar to [defining audit rules](#) and includes the following basic steps:

- Specify which events will trigger alert notifications. You can enable notification of successful and/or failed attempts to access a device. Select the **Alert Allowed** check box to enable notification of successful attempts to access a device. Select the **Alert Denied** check box to enable notification of failed attempts to access a device.
- Specify users and/or groups whose actions will trigger alert notifications. To do so, in the upper-left pane of the dialog box, under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.
- Specify which user's actions on devices either will or will not trigger alert notifications. In the upper-left pane of the dialog box, under **Users**, select the user or group that you added. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny an alert right. Alert rights determine which user actions on devices trigger alert

notifications. Alert rights are identical to audit rights. The only difference is that when events matching specific criteria occur DeviceLock triggers alerts instead of logging these events in the Audit Log. For a list of Audit rights for devices, see [“Audit” Rights Category](#).

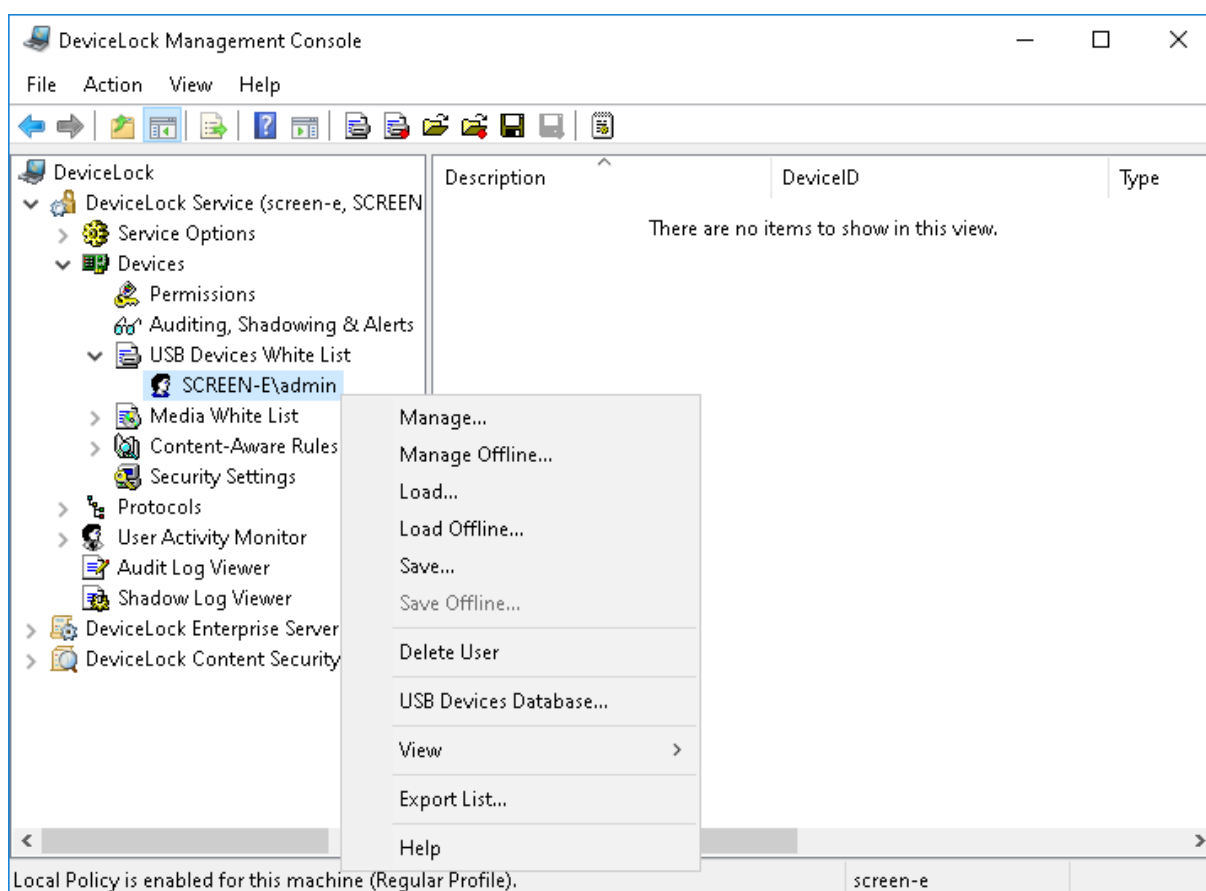
- Specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user’s actions on devices either will or will not trigger alert notifications. To do so, in the right pane of the dialog box, use the left mouse button to select days and hours when the selected user’s actions on devices will trigger alert notifications. Use the right mouse button to mark days and hours when the selected user’s actions on devices will not trigger alert notifications.

## Note

You can enable different online vs. offline device type-specific alerts. Online alerts (Regular Profile) are generated when client computers are working online. Offline alerts (Offline Profile) are generated when client computers are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to enable offline alerts, see [Managing Offline Audit, Shadowing and Alerts for Devices](#).

## USB Devices White List (Regular Profile)

The devices white list allows you to authorize only specific devices that will not be locked regardless of any other settings. The intention is to allow special devices but lock all other devices.



In the console tree you can see a list of users and groups that have a devices white list specified. Devices in the white list can be specified individually for every user and group. For more information on how the devices white list works, refer to the [Managed Access Control](#) section of this manual.

The shortcut menu of the devices white list provides the following commands:

- **Delete User** - Deletes the user or group from the white list along with all devices assigned to that user or group.
- **Manage** - Opens a dialog box where you can set or change the online (regular) white list.
- **Manage Offline** - Opens a dialog box where you can set or change the offline white list.
- **Load** - Loads a previously saved regular white list from an external file.
- **Load Offline** - Loads a previously saved offline white list from an external file.
- **Save** - Saves the regular white list to an external file.
- **Save Offline** - Saves the offline white list to an external file.
- **Undefine** - Resets the entire regular white list to the unconfigured state. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Undefine Offline** - Resets the entire offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.
- **Remove Offline** - Blocks the inheritance of the offline white list and enforces the regular white list. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **USB Devices Database** - Opens a dialog box where you can add devices to the USB Devices Database, making them available for adding to the white list.

---

#### Note

You can define different online vs. offline USB Devices White Lists for the same user or sets of users. The online USB Devices White List (Regular Profile) applies to client computers that are working online. The offline USB Devices White List (Offline Profile) applies to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define the offline USB Devices White List, see [Managing Offline USB Devices White List](#).

---

There are two ways to identify devices in the white list:

- **Device Model** - Represents all devices of the same model. Each device is identified by a combination of Vendor ID (VID) and Product ID (PID).  
This combination of VID and PID describes a unique device model but not a unique device unit. It means that all devices belonging to the certain model of the certain vendor will be recognized as the one authorized device.
- **Unique Device** - Represents a unique device unit. Each device is identified by a combination of Vendor Id (VID), Product Id (PID) and Serial Number (SN).  
Not all devices have serial numbers assigned. A device can be added to the white list as a **Unique Device** only if its manufacturer has assigned a serial number to it at the production stage.

Two steps are required to authorize a device:

1. Add the device to the devices database (see [USB Devices Database](#)), making it available for adding to the white list.
2. Add the device to the white list for the specified user/group. In effect, this designates the device as authorized and allows it for this user/group at the interface (USB) level.

---

**Note**

Audit is not performed for users' attempts to access a white-listed device while users' attempts to insert or remove a white-listed device are audited.

---

## White-Listed Devices

When you select a user or group under the **USB Devices White List** node in the console tree, the details pane lists the devices included in the white list for that user or group.

The shortcut menu on a device in the details pane provides the following commands:

- **Manage** - Depending on whether the device is in the regular or offline white list, opens a dialog box that allows you to define the online (regular) or offline USB Devices White List.
- **USB Devices Database** - Opens a dialog box where you can add devices to the USB Devices Database, making them available for adding to the white list.
- **Reinitialize** - Select this flag to force the white-listed device to reinitialize (replug) when a new user logs in. Some USB devices (such as the mouse) cannot work without reinitializing, so it is recommended to select this flag for non-storage devices. It is also advisable to clear this flag for data storage devices (flash drives, optical drives, external hard drives, etc.).

---

**Important**

DeviceLock Service can't reinitialize USB devices whose drivers do not provide for software replug of device. If there is no access to such a device from the white list, the user must remove the device from the USB port and then insert it back to restart the driver.

---

- **Control As Type** - When this flag is selected, access control for white-listed devices is disabled only at the interface (USB) level. If the white-listed device (e.g. USB Flash Drive) belongs to both levels: interface (USB) and type (Removable), the permissions as well as auditing, shadowing and alerts settings (if any) for the type level will be applied anyway. Otherwise, if this flag is cleared, access control at the type level is also disabled. For example, by clearing the **Control As Type** flag for a USB Flash Drive you can bypass security checking at the Removable device type level.
- **Read-only** - When this flag is selected, only read access to the white-listed storage device is allowed. If the device doesn't support read-only access then access to the device is blocked.
- **Allow Audit & Shadowing as Type** - Enables auditing, shadowing and alerting for the white-listed device at the type level according to settings defined in Auditing, Shadowing & Alerts, for all device types this device belongs to.
- **Delete** - Deletes the device from the white list of the user or group selected in the console tree.

### **Recommendations**

Attempts to use a removable device added to the USB Devices White List may fail with the “Access is denied” error. This issue is usually because the user does not have permission for removable devices. Note that permission check for removable USB devices is performed at both the interface level (USB port) and type level (Removable). If the user is not allowed to use removable devices, whitelisting such a device will not suffice unless permission control by device type is disabled in the white list.

To resolve the issue, grant the user permission to access removable devices (for instructions on how to set permissions, see [Permissions \(Regular Profile\)](#)), or clear the **Control As Type** flag for the given whitelisted device.

If the same device is added to the white list for different users, then changing the **Control As Type** flag for this device for one of the users will change it for all users as well. The **Control As Type** and **Reinitialize** flags apply to devices, not users, so changing them affects all users for whom this device is whitelisted.

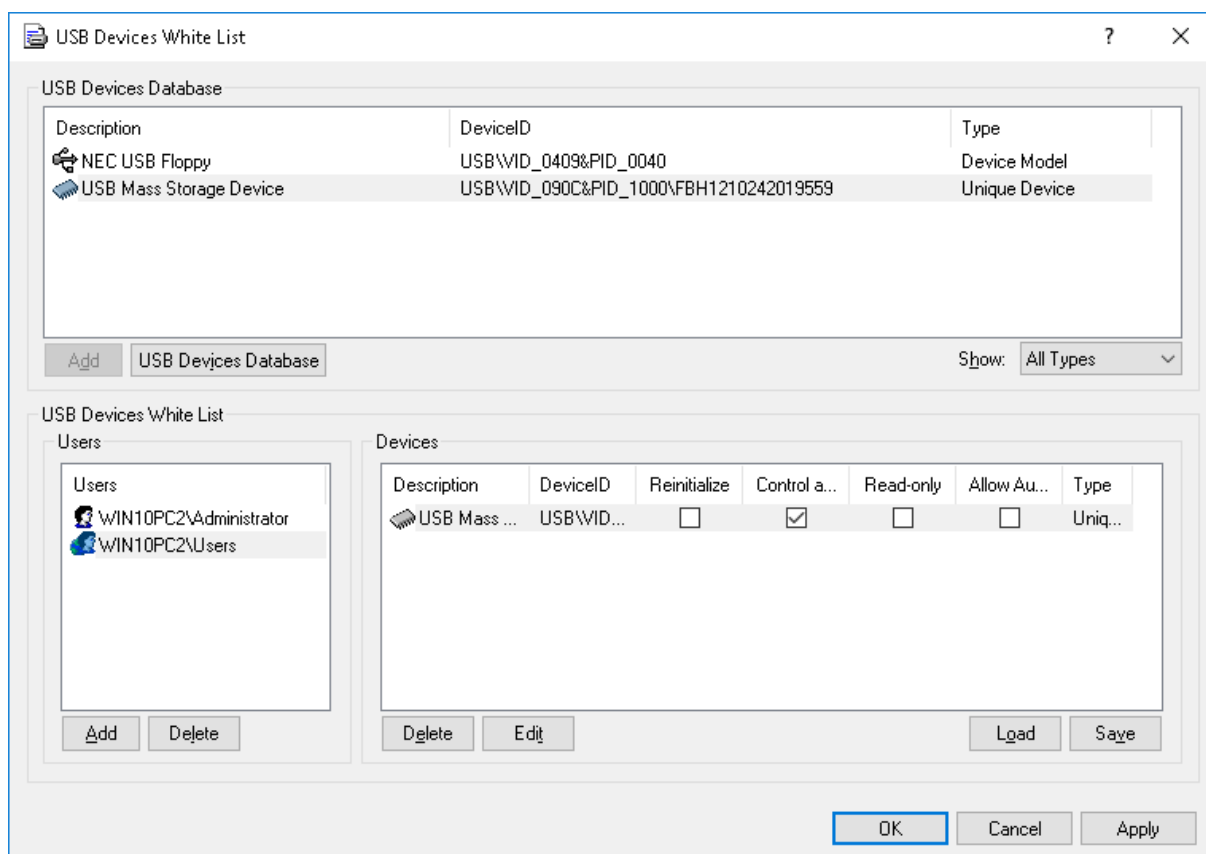
It is not possible to set the **Control As Type** flag differently for different users of the same device. As a workaround, you can define the device as unique for some users and define it as a model for others (for more information on identifying USB devices, see [Device Model vs. Unique Device](#)). In this way, you can create two white list entries for the same device with different **Control As Type** flag settings.

## USB Devices White List Dialog Box

To define the online (regular) white list, select **Manage** from the shortcut menu available with a right mouse click. Alternatively, you can click the appropriate button on the toolbar.

In the **USB Devices Database** list at the top of the dialog box, you can see devices that were added to the database.





Once devices are added from the database to the white list of a certain user, they become authorized devices for which access control is disabled when this user is logged in.

You can add a device to the USB Devices White List in two steps:

1. Select a user or user group for which this device should be allowed. Click **Add** under the **Users** list to add the user/group. To delete the record from the **Users** list, click **Delete**.
2. Select the appropriate device record in the **USB Devices Database** list and click **Add**.  
*If the device has an assigned serial number, it can be added to the white list two times: as Device Type and as Unique Device. In this case Device Type has a priority over Unique Device.*

When the **Control as Type** check box is selected, access control for white listed devices is disabled only on the interface (USB) level. If the white listed device (for example, USB Flash Drive) belongs to both levels: interface (USB) and type (Removable), the permissions as well as audit, shadowing and alert settings (if any) specified at the type level will be applied anyway.

Otherwise, if the **Control as Type** check box is not selected, access control at the type level is also disabled. For example, by clearing the **Control as Type** check box for a USB flash drive you disable the checking of access permissions on that drive that are specified for the Removable device type.

---

**Note**

When adding a USB composite device (one represented in the system as a parent device and one or more child devices) to the USB Devices White List, consider the following:

- If any device of a USB composite device is in the white list, access control is disabled for all devices of the composite device at the interface (USB port) level. In this case, if the white-listed device belongs to both levels: interface (USB) and type (for example, Removable), and the **Control as Type** check box is selected, the permissions (if any) specified at the type level will be applied anyway.
- 

When the **Read-only** check box is selected, only read access is granted to the white listed storage device. If this device doesn't support read-only access then access to this device is blocked.

Select the **Allow Audit & Shadowing as Type** check box to enable auditing, shadowing and alerting for a white-listed device at the type level according to the settings defined in Auditing, Shadowing & Alerts, for all device types this device belongs to.

Select the **Reinitialize** check box to force the white-listed device to reinitialize (replug) when a new user logs in. Some USB devices (such as the mouse) cannot work without reinitializing, so it is recommended to select this check box for non-storage devices. It is also advisable to clear this check box for data storage devices (flash drives, optical drives, external hard drives, etc.).

---

**Important**

DeviceLock Service cannot reinitialize USB devices whose drivers do not provide for software replug of device. If there is no access to such a device from the white list, the user should remove the device from the USB port and then insert it back to restart the driver.

---

To edit a device's description, select the appropriate record in **USB Devices White List** and click **Edit**.

---

**Note**

By default, the console checks the uniqueness of each USB device description, prompting to change the description if needed. You can opt out of this check by adding the following registry value on the computer running the console:

- Key: HKEY\_CURRENT\_USER\Software\SmartLine Vision\DLManager\Manager
  - Value: DisableWLNameUniquenessCheck=dword:00000001
- 

Click **Delete** to delete a selected device's record (use CTRL and/or SHIFT to select several records simultaneously).

To save the white list to an external file, click **Save**, and then select the name of the file. To load a previously saved white list, click **Load** and select a file that contains the list of devices.

If you need to manage the devices database (see [USB Devices Database](#)), you can click **USB Devices Database** and open the respective dialog box.

## Note

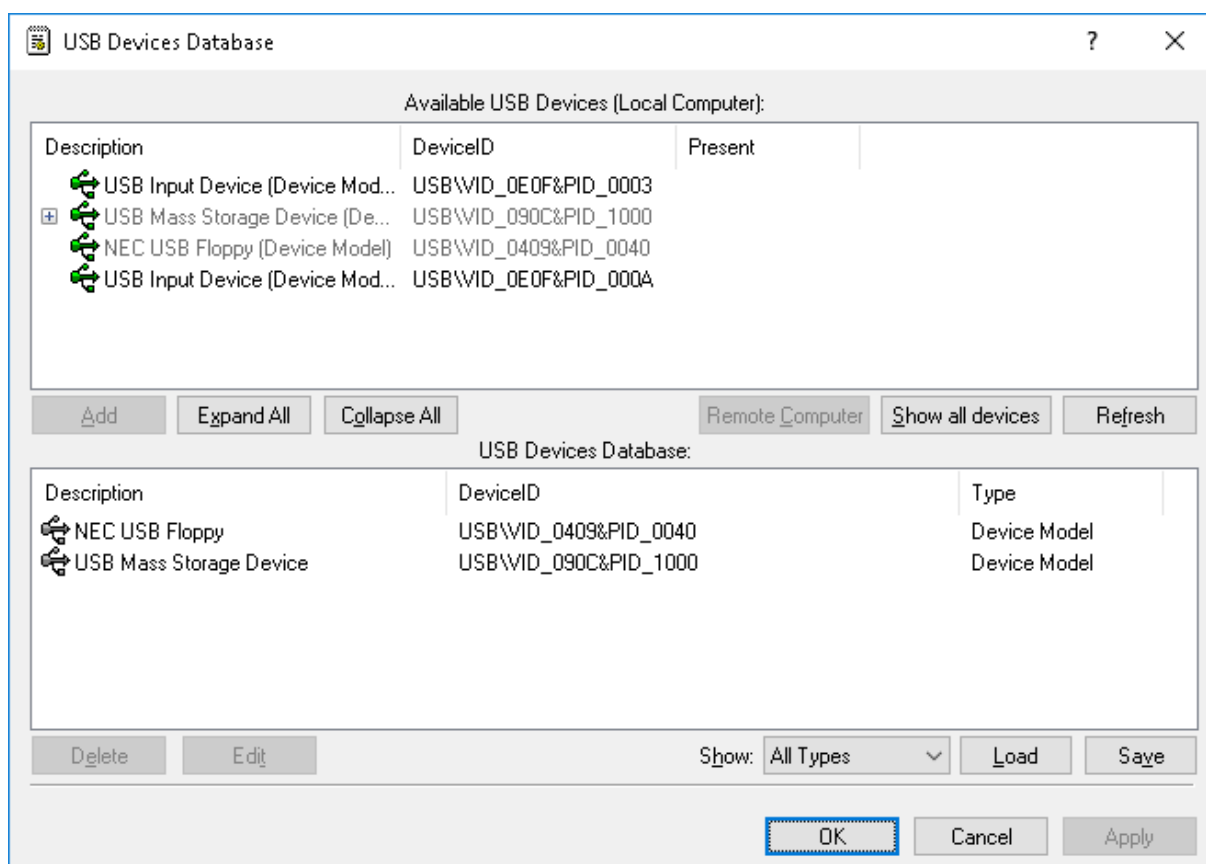
If you add an iPhone device to the USB Devices White List, access control is disabled for both the iPhone and its camera at the interface (USB port) level. Thus, you cannot allow access to iPhone and deny access to its camera at the interface (USB port) level. In the USB devices database, an iPhone device is identified as the Apple Mobile Device USB Driver.

However, it is possible to allow access to iPhone's camera and deny access to iPhone. To do this, you can use any of the following methods:

- Method 1. To allow access to iPhone's camera, add the iPhone to the USB Devices White List and select the **Control as Type** check box. To deny access to iPhone, set the "No Access" permission for the iPhone device type.
- Method 2. To allow access to iPhone's camera, clear the **Access control for USB scanners and still image devices** check box in **Security Settings**. To deny access to iPhone, set the "No Access" permission for the USB port device type.

## USB Devices Database

In the **USB Devices Database** dialog box you can add new devices to the database and edit existing records. Before the device can be authorized in the white list (see [USB Devices White List \(Regular Profile\)](#)), it must be added to the database.



In the **Available USB Devices** list at the top of the dialog box, you can see all devices available on the computer. Devices are displayed in the form of a simple tree, where the parent item represents **Device Model** and the child item represents **Unique Device**. If there is no Unique Device item, then this device does not have an assigned serial number.

This list displays either all currently plugged-in devices (if the **Show all devices** button is not clicked) or all the devices ever plugged into the port on this computer (if the **Show all devices** button is clicked).

The list of available devices is automatically refreshed and displays new devices as soon as they arrive. To manually refresh this list, click **Refresh**.

To retrieve devices from the remote computer, click **Remote Computer**. This button is unavailable when you are connected to the local computer.

In the **USB Devices Database** list at the bottom of the dialog box, you can see devices that are already in the database. You can add devices to this list by selecting the desired device's record in the **Available USB Devices** list and clicking **Add**. If the device is already in the database, it cannot be added there a second time.

To change the description of a device, select it in the **USB Devices Database** list and click **Edit**.

---

#### Note

By default, the console checks the uniqueness of each USB device description, prompting to change the description if needed. You can opt out of this check by adding the following registry value on the computer running the console:

- Key: HKEY\_CURRENT\_USER\Software\SmartLine Vision\DLManager\Manager
- Value: DisableWLNameUniquenessCheck=dword:00000001

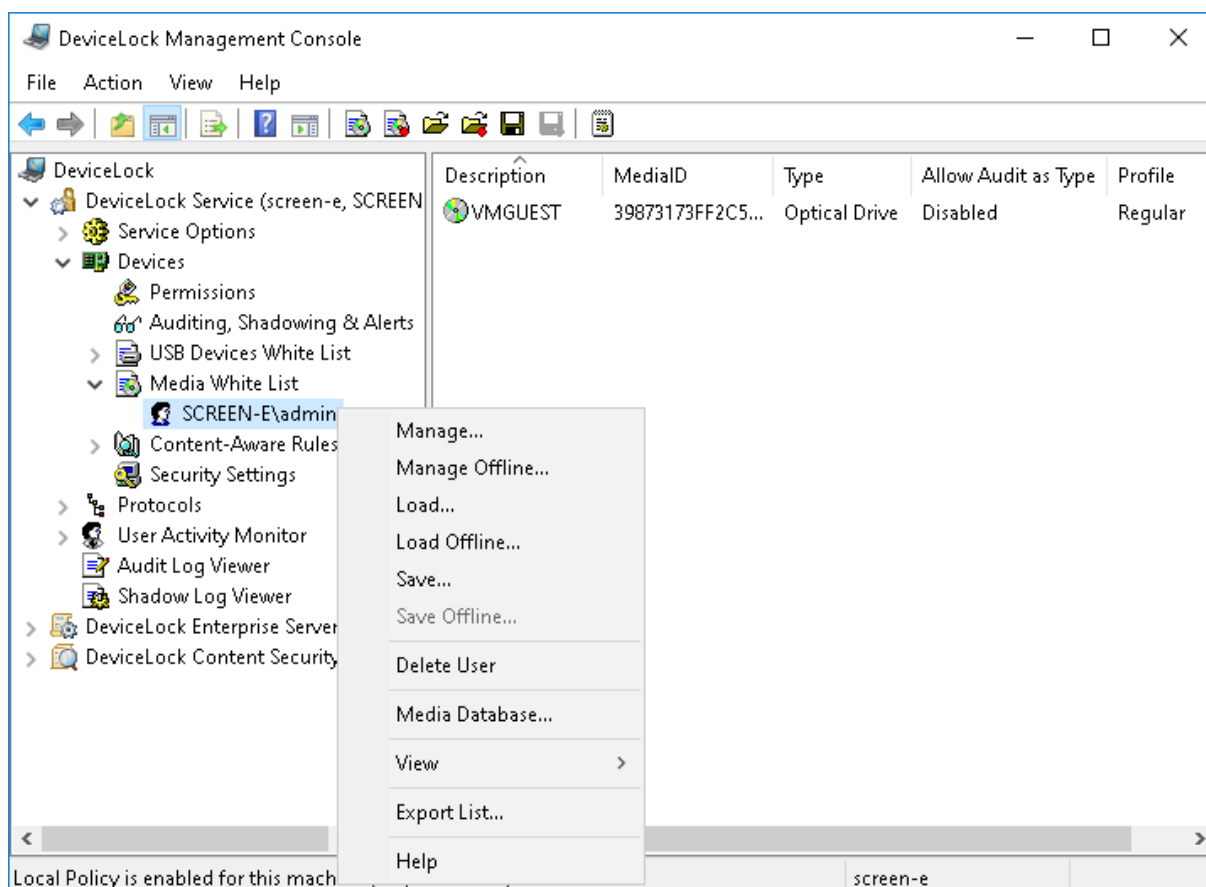
---

Click **Delete** to delete a selected device's record (press CTRL and/or SHIFT to select several records simultaneously).

You can also save a current database to an external file. To save the database to a file, click **Save**, then select the type of the file: either .txt or .csv. To load a previously saved database, click **Load** and select a file that contains the list of devices.

## Media White List (Regular Profile)

The media white list allows you to uniquely identify a specific CD/DVD/BD-ROM disk by the data signature and authorize read access to it, even when DeviceLock Service has otherwise blocked optical drives.



In the console tree you can see a list of users and groups that have a media white list specified. Media in the white list can be specified individually for every user and group.

The shortcut menu of the media white list provides the following commands:

- **Delete User** - Deletes the user or group from the white list along with all media assigned to that user or group.
- **Manage** - Opens a dialog box where you can set or change the online (regular) white list.
- **Manage Offline** - Opens a dialog box where you can set or change the offline white list.
- **Load** - Loads a previously saved regular white list from an external file.
- **Load Offline** - Loads a previously saved offline white list from an external file.
- **Save** - Saves the regular white list to an external file.
- **Save Offline** - Saves the offline white list to an external file.
- **Undefine** - Resets the entire regular white list to the unconfigured state. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Undefine Offline** - Resets the entire offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.
- **Remove Offline** - Blocks the inheritance of the offline white list and enforces the regular white list. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Media Database** - Opens a dialog box where you can add media to the Media Database, making them available for adding to the white list.

---

**Note**

You can define different online vs. offline Media White Lists for the same user or sets of users. The online Media White List (Regular Profile) applies to client computers that are working online. The offline Media White List (Offline Profile) applies to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define the offline Media White List, see [Managing Offline Media White List](#).

---

The media white list can be configured to grant access to a collection of approved CD/DVD/BD-ROM disks by certain users and groups, so that only authorized users are able to use the approved information.

Any change to the content of the media will change the data signature, thus invalidating authorization. If the user copies the authorized media without any changes in the original content (byte-to-byte copy) then such a copy is accepted as the authorized media.

Two steps are required to authorize media:

1. Add the media to the database (see [Media Database](#)), making it available for adding to the white list.
2. Add the media to the white list for the specified user/group. In effect, this designates the media as authorized and allows it (read access) for this user/group at the type (Optical Drive) level.

---

**Note**

Access to white listed media can be granted only on the type (Optical Drive) level. If the CD/DVD/BD drive plugs into the port (USB or FireWire) and access to this port is denied, then access to the white listed media is denied too.

---

## White-Listed Media

When you select a user or group under the **Media White List** node in the console tree, the details pane lists the media included in the white list for that user or group.

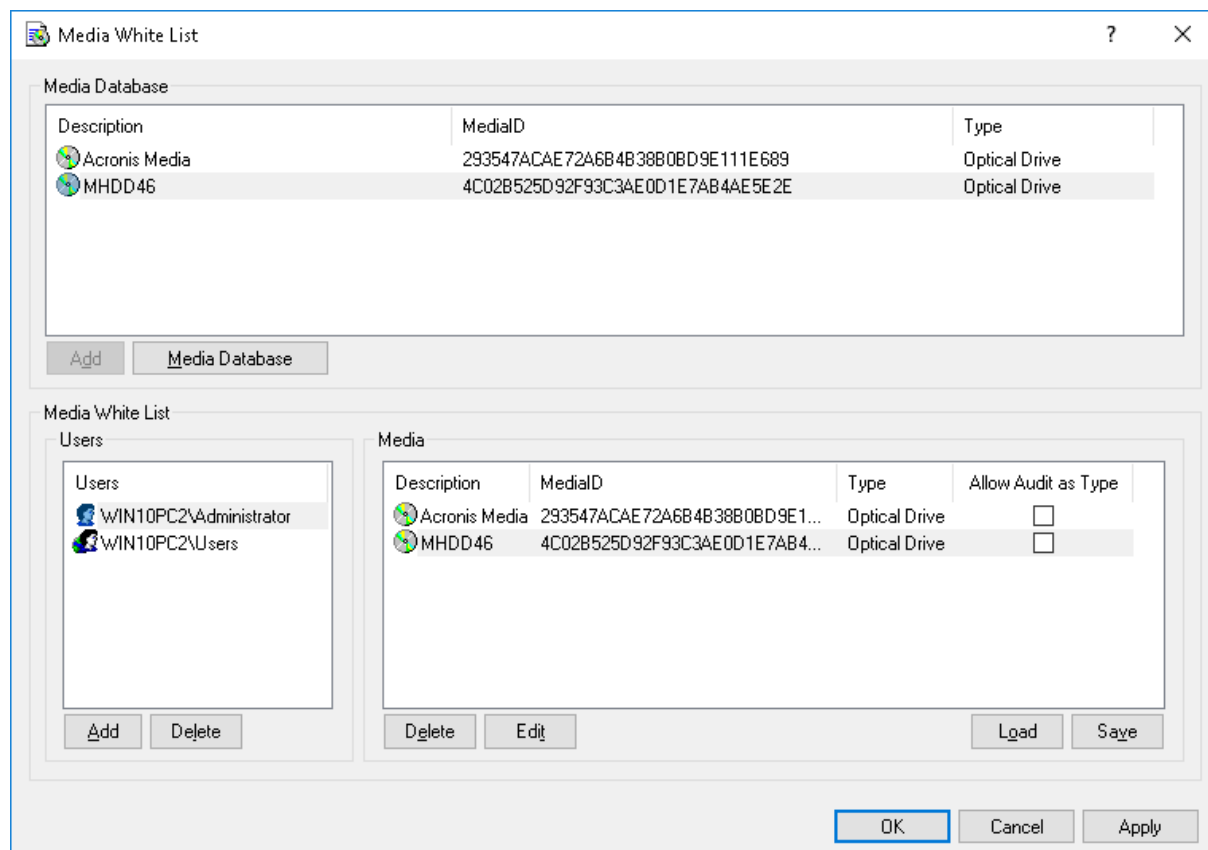
The shortcut menu on a media in the details pane provides the following commands:

- **Manage** - Depending on whether the media is in the regular or offline white list, opens a dialog box that allows you to define the online (regular) or offline Media White List.
- **Media Database** - Opens a dialog box where you can add media to the Media Database, making them available for adding to the white list.
- **Allow Audit as Type** - Enables auditing and alerting for the white-listed media at the type level according to settings defined in Auditing, Shadowing & Alerts for the Optical Drive device type.
- **Delete** - Deletes the media from the white list of the user or group selected in the console tree.

## Media White List Dialog Box

To define the online (regular) media white list, select **Manage** from the shortcut menu available with a right mouse click. Alternatively, you can click the appropriate button on the toolbar.

In the **Media Database** list at the top of the dialog box, you can see all media that were added to the database.



Once media are added from the database to the white list of a certain user, they become authorized media for which access control is disabled when this user is logged in.

You can add media to the Media White List in two steps:

1. Select a user or user group for which this media should be allowed. Click **Add** under the **Users** list to add the user/group. To delete the record from the **Users** list, click **Delete**.
2. Select the appropriate media record in the **Media Database** list and click **Add**.

Select the **Allow Audit as Type** check box to enable auditing and alerting for the white listed media according to the settings defined in [Auditing, Shadowing & Alerts \(Regular Profile\)](#) for the **Optical Drive** device type.

To edit a media's description, select the appropriate record in **Media White List** and click **Edit**.

---

**Note**

By default, the console checks the uniqueness of each media description, prompting to change the description if needed. You can opt out of this check by adding the following registry value on the computer running the console:

- Key: HKEY\_CURRENT\_USER\Software\SmartLine Vision\DLManager\Manager
  - Value: DisableWLNameUniquenessCheck=dword:00000001
- 

Click **Delete** to delete a selected media's record (use CTRL and/or SHIFT to select several records simultaneously).

To save the media white list to an external file, click **Save**, then select the name of the file. To load a previously saved white list, click **Load** and select a file that contains the list of medias.

If you need to manage the media database (see [Media Database](#)), you can click **Media Database** and open the appropriate dialog box.

---

**Note**

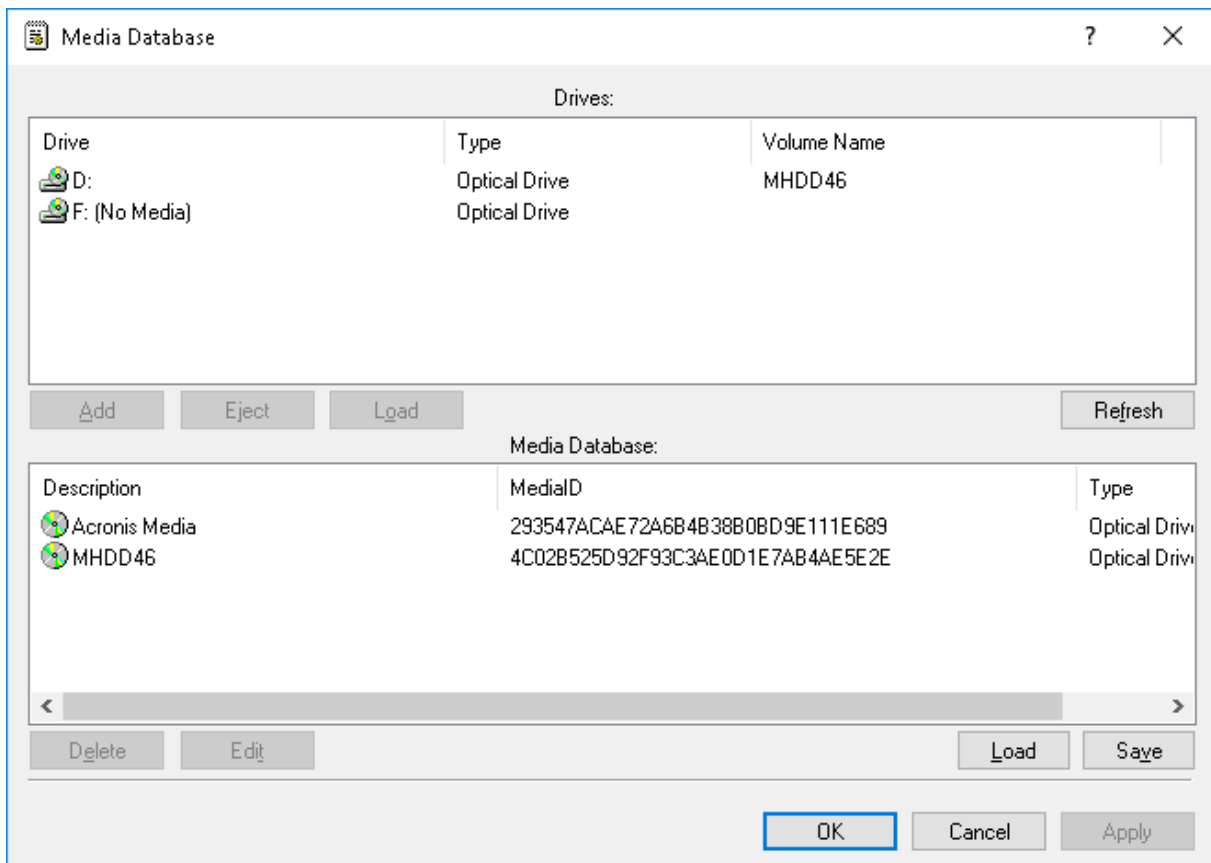
Using the media white list you can only allow read access to authorized media. It is impossible to authorize media for writing.

---

## Media Database

In the **Media Database** dialog box you can add new media to the database and edit existing records.





Before the media can be authorized in the white list (see [Media White List \(Regular Profile\)](#)), it must be added to the database.

In the **Drives** list at the top of the dialog box, you can see all drives available on the local computer that can contain medias.

The list is automatically refreshed and displays new medias as soon as they arrive. To manually refresh this list, click **Refresh**.

In the list at the bottom of the dialog box, you can see media that are already in the database.

You can add media to this list by selecting the desired record in the **Drives** list and clicking **Add**. It takes some time (depending on the media size) to authorize the media. If the media is already in the database, it cannot be added there a second time.

To edit a media's description, select the appropriate record in the list and click **Edit**.

### Note

By default, the console checks the uniqueness of each media description, prompting to change the description if needed. You can opt out of this check by adding the following registry value on the computer running the console:

- Key: HKEY\_CURRENT\_USER\Software\SmartLine Vision\DLManager\Manager
- Value: DisableWLNameUniquenessCheck=dword:00000001

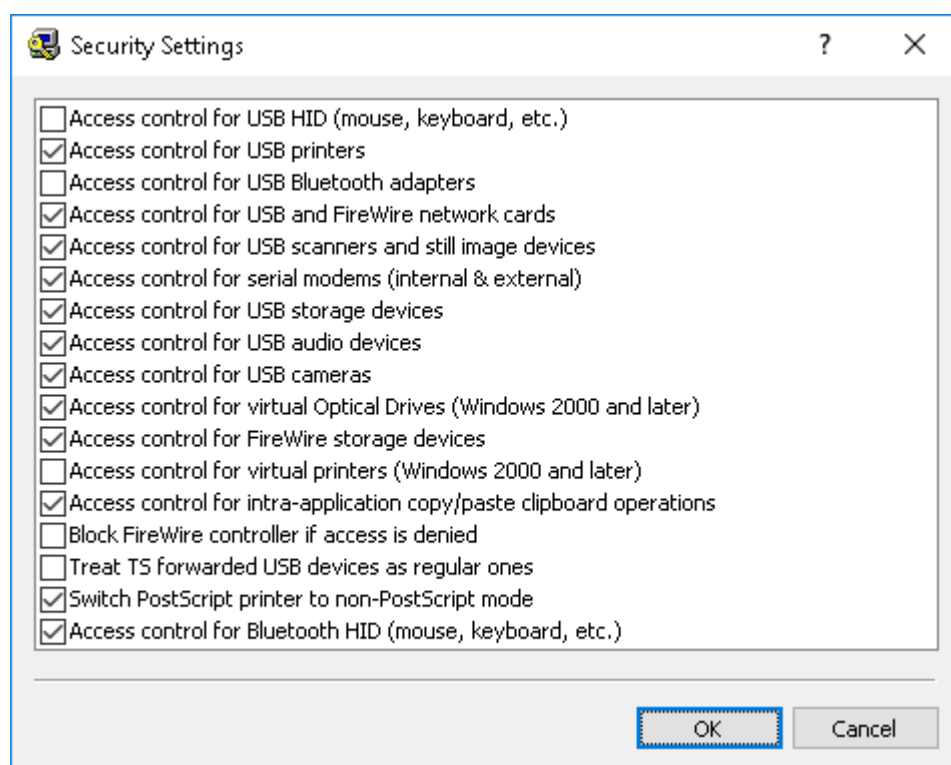
Click **Delete** to delete a selected record (use CTRL and/or SHIFT to select several records simultaneously).

You can also save a current database to an external file. To save the database to an external file, click **Save**, then select the type of the file: either .txt or .csv.

To load a previously saved database, click **Load** and select a file that contains the list of media.

## Security Settings (Regular Profile)

DeviceLock provides a number of additional security parameters that affect permissions and audit rules for certain device types. These security parameters provide the ability to keep some device types completely locked, but allow the use of certain device classes without the need to authorize every device in the white list. For example, you can disallow the use of all USB devices except any mouse and keyboard devices that connect through the USB. For further details, see [Security Settings Description](#).



## Security Settings Node

This node in the console tree is intended to administer security settings for devices (see [Security Settings Description](#) later in this document).

The shortcut menu on the **Security Settings** node provides the following commands:

- **Manage** - Opens a dialog box where you can enable or disable regular (online) security settings collectively.

- **Manage Offline** - Opens a dialog box where you can enable or disable offline security settings collectively.

---

#### Note

You can define different online vs. offline security settings for the same user or sets of users. Online security settings (Regular Profile) apply to client computers that are working online. Offline security settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define offline security settings, see [Managing Offline Security Settings for Devices](#).

---

When you select the **Security Settings** node, a list of settings appears the details pane. To manage a setting, right-click it in the details pane and use commands from the shortcut menu:

- **Enable** - Enables the online (regular) security setting.
- **Disable** - Disables the online (regular) Security Setting.
- **Undefine** - Resets the regular security setting to the unconfigured state. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Enable Offline** - Enables the offline security setting.
- **Disable Offline** - Disables the offline security setting.
- **Undefine Offline** - Resets all the previously defined offline security settings to the unconfigured state. If offline security settings are undefined, regular security settings are applied to offline client computers.
- **Manage** - Opens a dialog box where you can enable or disable regular (online) security settings collectively.
- **Manage Offline** - Opens a dialog box where you can enable or disable offline security settings collectively.
- **Remove Offline** - Blocks the inheritance of offline security settings and enforces regular security settings. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).

To change online (regular) security setting, you can double-click the setting in the details pane to switch its state (**enable/disable**). Alternatively, you can choose the **Manage** command from the shortcut menu or click the appropriate button on the toolbar.

## Security Settings Description

DeviceLock provides the following security settings for devices:

- **Access control for USB HID** - If enabled, allows DeviceLock Service to audit and control access to Human Interface Devices (mouse, keyboard, and so on) plugged into the USB port. Otherwise, even if the USB port is locked, Human Interface Devices continue to function as usual and audit is not performed for these devices.

- **Access control for USB printers** - If enabled, allows DeviceLock Service to audit and control access to printers plugged into the USB port. Otherwise, even if the USB port is locked, printers continue to function as usual and audit is not performed for these devices.
- **Access control for USB scanners and still image devices** - If enabled, allows DeviceLock Service to audit and control access to scanners and still image devices plugged into the USB port. Otherwise, even if the USB port is locked, these devices continue to function as usual and audit is not performed for these devices.
- **Access control for USB Bluetooth adapters** - If enabled, allows DeviceLock Service to audit and control access to Bluetooth adapters plugged into the USB port. Otherwise, even if the USB port is locked, Bluetooth adapters continue to function as usual and audit is not performed for these devices.  
*This parameter affects audit and access control on the interface (USB) level only. If the device belongs to both levels, the permissions and audit rules (if any) for the type (Bluetooth) level will be applied anyway.*
- **Access control for USB storage devices** - If enabled, allows DeviceLock Service to audit and control access to storage devices (such as flash drives) plugged into the USB port. Otherwise, even if the USB port is locked, storage devices continue to function as usual and audit is not performed for these devices.  
*This parameter affects audit and access control on the interface (USB) level only. If the device belongs to both levels: interface and type, the permissions and audit rules (if any) for the type (Removable, Floppy, Optical Drive or Hard disk) level will be applied anyway.*
- **Access control for USB audio devices** - If enabled, allows DeviceLock Service to audit and control access to audio devices (such as headsets and microphones) plugged into the USB port. Otherwise, even if the USB port is locked, these devices continue to function as usual and audit is not performed for these devices.
- **Access control for USB cameras** - If enabled, allows DeviceLock Service to audit and control access to Web cameras plugged into the USB port. Otherwise, even if the USB port is locked, these devices continue to function as usual and audit is not performed for these devices.
- **Access control for USB and FireWire network cards** - If enabled, allows DeviceLock Service to audit and control access to network cards plugged into the USB or FireWire (IEEE 1394) port. Otherwise, even if the USB or FireWire port is locked, network cards continue to function as usual and audit is not performed for these devices.
- **Access control for FireWire storage devices** - If enabled, allows DeviceLock Service to audit and control access to storage devices plugged into the FireWire port. Otherwise, even if the FireWire port is locked, storage devices continue to function as usual and audit is not performed for these devices.  
*This parameter affects audit and access control on the interface (FireWire) level only. If the device belongs to both levels: interface and type, the permissions and audit rules (if any) for the type (Removable, Floppy, Optical Drive or Hard disk) level will be applied anyway.*
- **Access control for serial modems (internal & external)** - If enabled, allows DeviceLock Service to audit and control access to modems plugged into the COM port. Otherwise, even if the COM

port is locked, modems continue to function as usual and audit is not performed for these devices.

- **Access control for virtual Optical Drives** - If enabled, allows DeviceLock Service to audit and control access to virtual (software emulated) CD/DVD/BD-ROMs. Otherwise, even if the CD/DVD/BD device is locked, virtual drives continue to function as usual and audit is not performed for these devices.
- **Access control for virtual printers** - If enabled, allows DeviceLock Service to audit and control access to virtual printers which do not send documents to real devices, but instead print to files (for example, PDF converters). Otherwise, even if the physical printer is locked, virtual printers continue to print as usual and audit is not performed for them.
- **Access control for intra-application copy/paste clipboard operations** - If enabled, allows DeviceLock Service to audit and control access to copy/paste operations within an application. Otherwise, even if the clipboard is locked, access control for copy/paste operations within one application is disabled and audit is not performed for them.
- **Block FireWire controller if access is denied** - If enabled, allows DeviceLock Service to disable FireWire controllers when the Everyone account has No Access permissions for the FireWire port device type.
- **Switch PostScript printer to non-PostScript mode** - If enabled, DeviceLock Service makes PostScript printers act like non-PostScript printers. This resolves an issue in which DeviceLock Service is unable to create a correct shadow copy of printed data and perform content analysis of data sent to printers that use a PostScript driver.
- **Treat TS forwarded USB devices as regular ones** - If enabled, allows DeviceLock Service to control access to all USB devices redirected during a Citrix XenDesktop/MS RemoteFX session according to the rights set for the USB port device type. Otherwise, DeviceLock Service controls access to all USB devices redirected during a Citrix XenDesktop/MS RemoteFX session according to the **USB Devices Access** right set for TS Devices.
- **Access control for Bluetooth HID** - If enabled, allows DeviceLock Service to audit and control access to Human Interface Devices (mouse, keyboard, and so on) connected via Bluetooth. Otherwise, even if Bluetooth is locked, Human Interface Devices continue to function as usual and audit is not performed for these devices.

*This parameter affects audit and access control on the type (Bluetooth) level only. If the device belongs to both levels: interface and type, the permissions and audit rules (if any) for the interface (USB) level will be applied anyway.*

Security Settings are similar to the device white list (see [USB Devices White List \(Regular Profile\)](#)) but there are three major differences:

1. Using Security Settings you can only allow a whole class of device. You cannot allow only a specific device model, while locking out all other devices of the same class.  
For example, by disabling **Access control for USB storage devices**, you allow the use of all USB storage devices, no matter their model and vendor. By specifying the one USB Flash Drive model you want to allow on the devices white list, you ensure that all other USB storage devices remain locked out.

2. Using Security Settings you can only select from the predefined device classes. If the device does not belong to one of the predefined classes, then it cannot be allowed.  
For example, there is no specific class for smart card readers in Security Settings, so if you want to allow a smart card reader when the port is locked, you should use the devices white list.
3. Security Settings cannot be defined on a per-user basis; they affect all users of the local computer. However, devices in the white list can be defined individually for the every user and group.

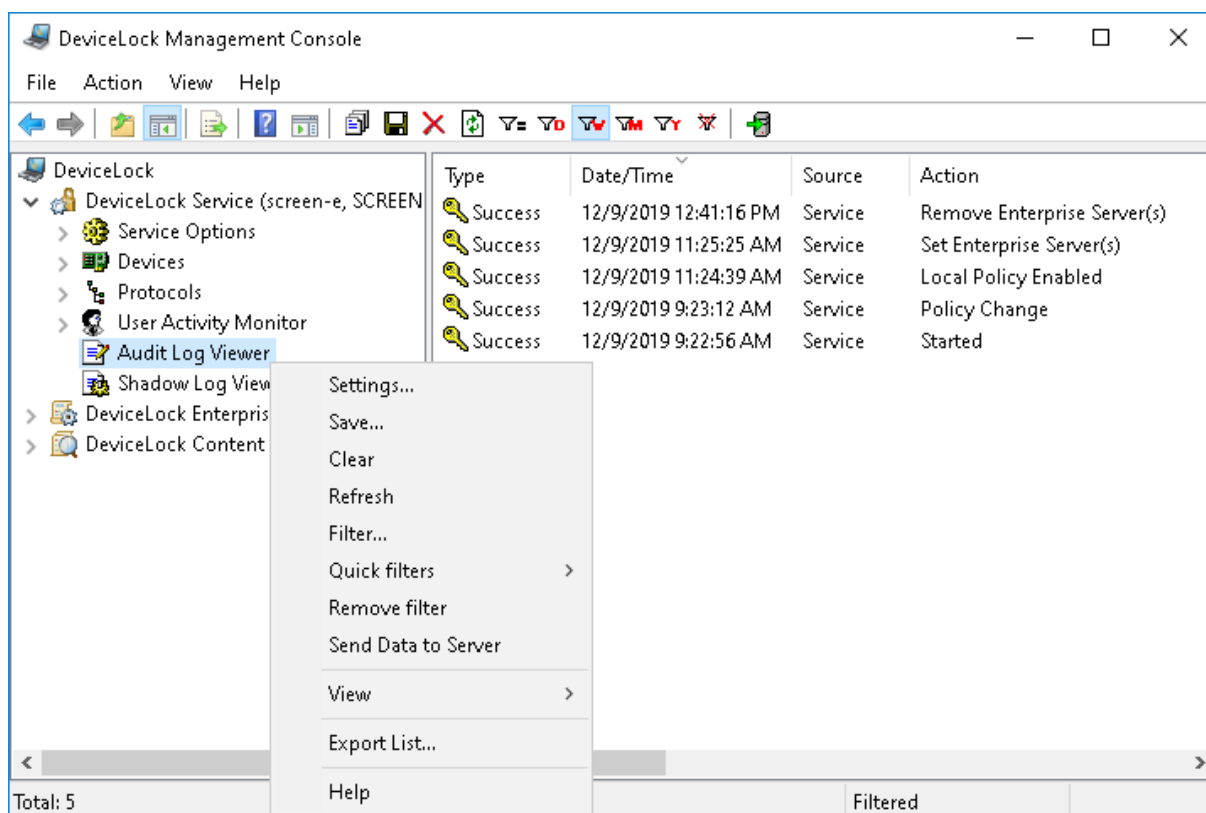
### Note

Security Settings work only for those devices that are using standard Windows drivers. Some devices are using proprietary drivers and their classes cannot be recognized by DeviceLock Service. Hence, access control to such devices cannot be disabled via Security Settings. In this case you may use the devices white list to authorize such devices individually (see [USB Devices White List \(Regular Profile\)](#)).

## Audit Log Viewer (Service)

There is a built-in audit log viewer that allows you to retrieve DeviceLock audit log records from a computer's local Windows event logging subsystem.

The standard Windows event logging subsystem is used to store audit records if **Event Log** is selected in the [Audit log type](#) parameter in [Service Options](#). If **DeviceLock Log** is selected, audit records are stored in the server log and can be viewed using the server's audit log viewer (see [Audit Log Viewer \(Server\)](#)).



The audit log stores events generated by a user's device-related activities that fall under the audit rules. For more information, refer to the [Auditing, Shadowing & Alerts \(Regular Profile\)](#) section of this manual.

Also, changes in a DeviceLock Service's configuration generate events in the audit log, if the [Log Policy changes and Start/Stop events](#) parameter is enabled in [Service Options](#).

The columns of this viewer are defined as follows:

- **Type** - The type of the event can be one of the following:
  - **Success** - DeviceLock has allowed a certain action, such as read, write or transfer a file or data.
  - **Failure** - DeviceLock has not allowed a certain action, such as read, write or transfer a file or data.
  - **Information** - DeviceLock has successfully applied a Content-Aware Rule for content detection.
  - **Warning** - DeviceLock encountered a condition that may cause a problem unless action is taken. A brief description of the issue or condition DeviceLock encountered can be found in the **Reason** or **Action** field.  
For instance, a warning can be caused by an issue that occurred when applying a Content-Aware Rule for content detection, as a result of which DeviceLock was unable to inspect the content of the file indicated in the **Name** field of the event record.
- **Date/Time** - The date and time that the event was received by DeviceLock Service.
- **Source** - The type of the device or protocol involved. Service can also be indicated as the source if the event is caused by an action that affects DeviceLock Service.
- **Action** - The action that caused the event.
- **Name** - The name of the object (file, USB device, etc.).
- **Information** - Other device- or protocol-specific information for the event, such as the access flags, the device or protocol name, device ID, device description from the [USB Devices Database](#), and so on.
- **Reason** - Indicates why the event occurred or what it was caused by. Possible values include:
  - **Device Permissions** - The event caused by an attempt to access, read or write data to a particular device.
  - **Protocol Permissions** - The event caused by an attempt to connect, send or receive data through a particular protocol.
  - **Security Settings** - The event caused by the triggering of a certain security setting for devices or protocols (see [Security Settings Description](#) for devices and [Security Settings Description](#) for protocols).
  - **Rule** - The event caused by the triggering of a certain Content-Aware Rule.  
This value is normally followed by the name of the rule and a brief description of the content matches, keywords, and/or file types that led to its triggering. For instance, if a rule employs a Keywords group, the description lists the words that the rule had reacted to.

If the rule failed to execute due to an error, a brief description of the error is provided, such as “DeviceLock Server unreachable”, “DeviceLock Server is too busy”, “Corrupted data” or “Password protected”.

- **White List** - The event caused either by a white-listed USB device, or by the triggering of a certain Protocol White List rule. This value is followed by the name of the respective device or rule.
- **IP Firewall** - The event caused by the triggering of a certain rule of the Basic IP Firewall. This value is followed by the name of the respective rule.
- **Content-Aware Rule error** - The event normally indicating that DeviceLock was unable to apply Content-Aware Rules to some file or data. As a result, the user was denied access to or transfer of that file or data.
- **Local Storage Quota Exceeded** - DeviceLock was unable to apply a rule to or create a shadow copy of some file or data because the size of the local storage directory has exceeded the local storage quota (for details, see [Local storage quota \(%\)](#)). As a result, the user was denied access to or transfer of the file or data.
- **Shadowing error** - DeviceLock was unable to create a shadow copy of some file or data due to an error accessing the local storage directory. As a result, the user was denied access to or transfer of the file or data.
- **Passthru** - The event caused by any of the following conditions:
  - A device removed from a USB port.
  - A removable device has been mounted or unmounted.
  - A connection to a remote host has been performed that services multiple web-based protocols, in a situation where protocol permissions allow connection to that host while other connections through HTTP are blocked. In this case, HTTP is indicated as the event source.
- **User** - The name of the user associated with this event.
- **PID** - The identifier of the process associated with this event.
- **Process** - The fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path.










## Managing the Audit Log (Service)

The log can be managed by using commands from the shortcut menu:

- In the DeviceLock Management Console tree, expand **DeviceLock Service**, and then right-click **Audit Log Viewer** under the **DeviceLock Service** node.  
- OR -
- In the DeviceLock Management Console tree, select **DeviceLock Service > Audit Log Viewer**, and then right-click any list record in the details pane.



The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):



- **Settings**  - View or change the settings that limit the maximum number of event records the log may contain (see [Audit Log Settings \(Service\)](#)).
- **Save**  - Save the log to the file you specify.
- **Clear**  - Delete all event records that currently exist in the log.  
This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.
- **Refresh**  - Update the list of events with the latest information.
- **Filter**  - Display only the events that match the conditions specified (see [Audit Log Filter \(Service\)](#)).
- **Quick filters** - Choose from the following options to view the events that occurred during:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

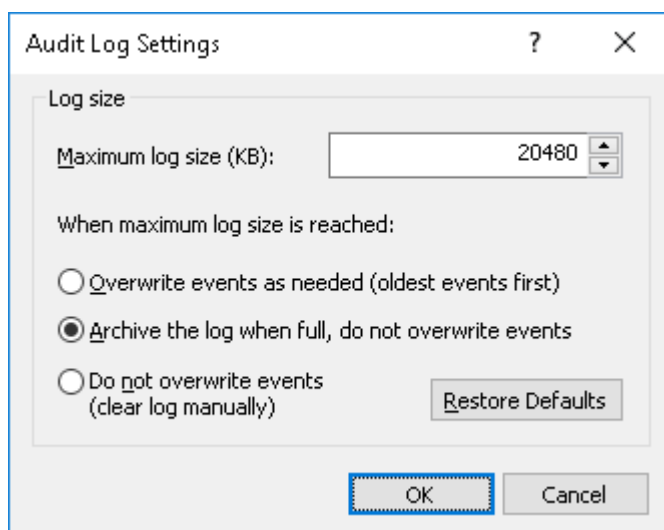
To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Send Data to Server**  - When the [DeviceLock Enterprise Server\(s\)](#) parameter is configured and the **DeviceLock Log** option is selected for the [Audit log type](#) parameter, the **Send Data to Server** command can be used to send log data to the DeviceLock Enterprise Server as soon as possible. Since the server collects log data automatically as it accumulates on the DeviceLock Service, the use of this command is optional.

## Audit Log Settings (Service)

To define a maximum log size and what Windows should do if the audit log becomes full, choose **Settings** from the shortcut menu of **Audit Log Viewer** or click  on the toolbar.



The **Maximum log size** parameter specifies the maximum size of the log file (in kilobytes). The log file is created and used only by the Windows Event Log service. Normally, this file is located in the folder %SystemRoot%\system32\config, and has the DeviceLo.evt name.

To specify what Windows should do when the event log is full (that is, when the maximum log size is reached), select one of these options:

- **Overwrite events as needed** - New events continue to be stored when the log is full. Each new incoming event replaces the oldest event in the log.
- **Archive the log when full, do not overwrite events** - The log is automatically archived when necessary. No events are overwritten.
- **Do not overwrite events (clear log manually)** - New events are not stored when the log is full. To store new events, the log must be cleared by hand.

If DeviceLock Service runs on Windows Server 2003, Windows XP or an earlier version of the Windows operating system, the following option appears instead of the option to archive the log when it is full:

- **Overwrite events older than <number> days** - New events replace only those events that are older than the specified number of days.

---

#### Note

When the event log is full and there are no records that Windows can overwrite, then DeviceLock Service is unable to write new audit records to this log.

---

To apply the default settings, click **Restore Defaults**. The default settings are as follows:

- The **Maximum log size** parameter is set to 20480 kilobytes.  
In case of Windows Server 2003, Windows XP or an earlier version of the Windows operating system, the **Maximum log size** parameter is set to 512 kilobytes.
- The **Archive the log when full, do not overwrite events** option is selected.


In case of Windows Server 2003, Windows XP or an earlier version of the Windows operating system, the **Overwrite events older than <number> days** option is selected with the number of days set to 7.

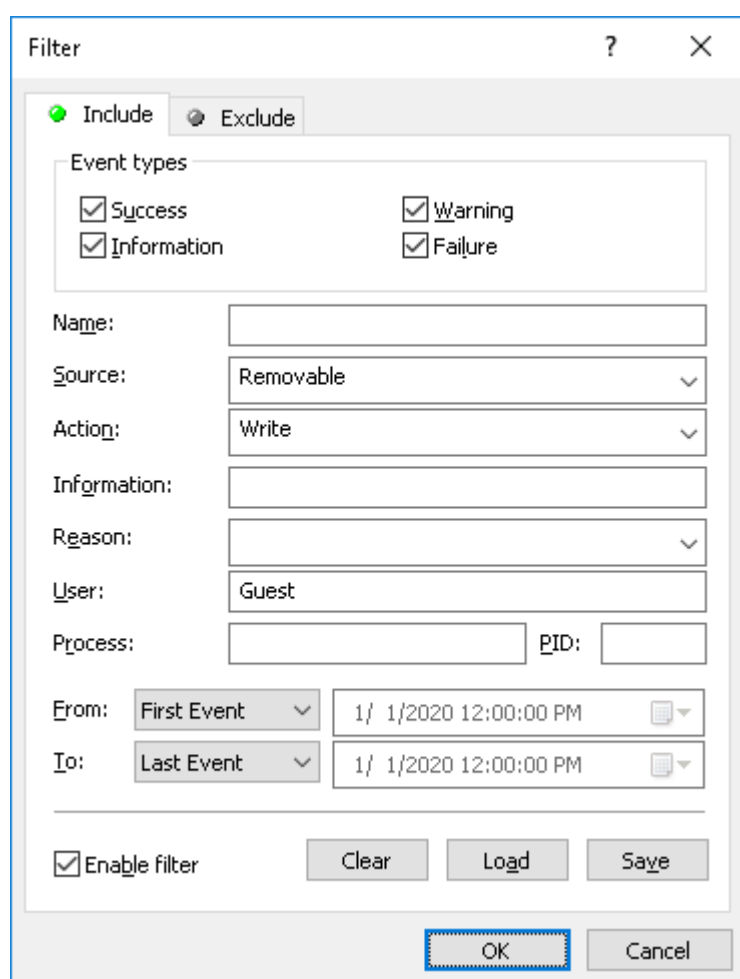
## Note

In the DeviceLock Service Settings Editor and DeviceLock Group Policy Manager consoles, regardless of the operating system version, the option **Overwrite events older than <number> days** is displayed instead of the option **Archive the log when full, do not overwrite events** and the default settings are as follows: the **Maximum log size** parameter is set to 512 kilobytes; the **Overwrite events older than <number> days** option is selected with the number of days set to 7.

## Audit Log Filter (Service)

You can filter data in [Audit Log Viewer \(Service\)](#) so that only records that meet specific conditions are displayed in the list.

To open the **Filter** dialog box, choose **Filter** from the shortcut menu of **Audit Log Viewer** or click  on the toolbar.



There are two types of filters:

- **Include** - Only the entries that match conditions specified on the **Include** tab are shown in the list.
- **Exclude** - The entries that match conditions specified on the **Exclude** tab are not shown in the list.

To use any filter, you should activate it first. Select the **Enable filter** check box to make a filter active. To temporary deactivate the filter, clear the **Enable filter** check box.

---

#### Note

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

When the filter is enabled, its conditions are defined by entering values in the following fields:

- **Event types** - Select check boxes to filter events by type:
  - **Success** - DeviceLock has allowed a certain action, such as read, write or transfer a file or data.
  - **Failure** - DeviceLock has not allowed a certain action, such as read, write or transfer a file or data.
  - **Information** - DeviceLock has successfully applied a Content-Aware Rule for content detection.
  - **Warning** - DeviceLock encountered a condition that may cause a problem unless action is taken.
- **Name** - The text that matches a value in the Audit Log Viewer's **Name** column. This field is case-insensitive.
- **Source** - The text that matches a value in the Audit Log Viewer's **Source** column. This field is case-insensitive.
- **Action** - The text that matches a value in the Audit Log Viewer's **Action** column. This field is case-insensitive.
- **Information** - The text that matches a value in the Audit Log Viewer's **Information** column. This field is case-insensitive.
- **Reason** - The text that matches a value in the Audit Log Viewer's **Reason** column. This field is case-insensitive.
- **User** - The text that matches a value in the Audit Log Viewer's **User** column. This field is case-insensitive.
- **Process** - The text that matches a value in the Audit Log Viewer's **Process** column. This field is case-insensitive and allows the use of wildcards.
- **PID** - The number that matches a value in the Audit Log Viewer's **PID** column. To enter multiple values, separate them with a semicolon (;).
- **From** - The beginning of the range of events to filter. Select **First Event** to filter events from the earliest one in the log. Select **Events On** to filter events that occurred no earlier than a specific date and time.
- **To** - The end of the range of events to filter. Select **Last Event** to filter events up to the latest one in the log. Select **Events On** to filter events that occurred no later than a specific date and time.

## Note

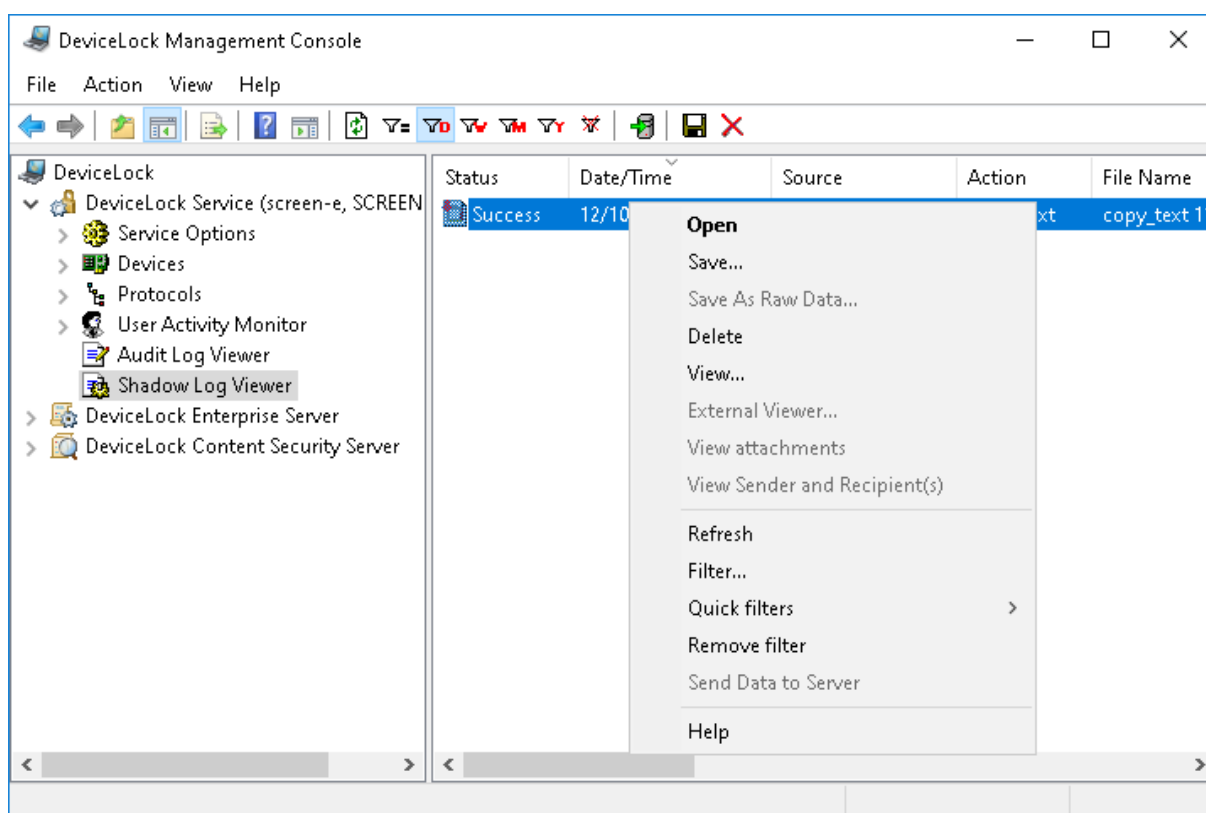
To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

## Shadow Log Viewer (Service)

There is a built-in shadow log viewer that allows you to retrieve the shadow log from DeviceLock Service.



The typical DeviceLock configuration assumes that the shadow data is stored on DeviceLock Enterprise Server. In this case all shadow data which is originally logged and cached by DeviceLock Service on the local computer is periodically moved to the server. The local shadow log is cleared as soon as the data is successfully moved to the server, so to view this data, you should use the server's shadow log viewer (see [Shadow Log Viewer \(Server\)](#)).

However, in some cases you may need to view the shadow log of a certain computer. This need arises when, for example, you do not use DeviceLock Enterprise Server at all or when the server is being used, but for some reason the data still exists on the client computer.

The columns of this viewer are defined as follows:

- **Status** - Indicates the status of the record:
  - **Success** - Data is successfully logged.
  - **Incomplete** - Data is possibly not completely logged.
  - **Failed** - Applies to shadow copies of files checked by Content-Aware Rules and whose transmission was blocked.

*If data transmission was blocked by permissions but was not checked by Content-Aware Rules, a shadow copy of the data is not created.*

- **Date/Time** - The date and the time when the data was transferred.
- **Source** - The type of device or protocol involved.
- **Action** - The user's activity type.
- **File Name** - The original path to the file or the auto-generated name of the data that originally was not a file (such as CD/DVD/BD images, data written directly to the media or transferred through the serial/parallel ports).
- **File Size** - The size of the data.
- **File Type** - The real file type of the file.

---

#### Note

When applied to files that have been transferred to Removable, Floppy, or Optical drive devices, this column is empty until a device or a disc the files were transferred to, are unplugged/removed.

---

- **Reason** - Indicates why the event occurred or what it was caused by. For details, see [description of this column in the audit log viewer](#).
- **Protected** - Indicates the protection status of a file. **Yes** status indicates that the file is protected. **No** status indicates that the file is not protected. Empty status indicates that the file is not protected, and does not have protection features. **Error** <text> status indicates an error during protection status detection has occurred.

---

### Note

Protection status can only be retrieved on Windows Vista or later operating systems. Retrieval attempts made on older operating systems result in the following error message in the Server log and Audit log: "Encryption Analyzer is not supported on this system."

---

- **Information** - Other device- or protocol-specific information for the event, such as the access flags, the device or protocol name, device ID, device description from the [USB Devices Database](#), and so on.
- **User** - The name of the user transferred the data.
- **PID** - The identifier of the process used to transfer the data.
- **Process** - Fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path.

## Managing Shadow Log Records

To manage Shadow Log records, use the shortcut menu available via a right mouse click on every record. The menu includes the following commands:

- [Open](#)
- [Save](#)
- [Save As Raw Data](#)
- [Delete](#)
- [View](#)
- [External Viewer](#)
- [View Attachments](#)
- [View Sender and Recipient\(s\)](#)

### Open


To open the file from a selected record with its associated application, use **Open** from the shortcut menu. If there is no associated application then the **Open With** dialog box is shown. In case the record has no associated data (its size is 0 or it was not logged), **Open** is disabled.

To enable EFS encryption of temporary files created when a shadow copy is opened/viewed, set the following registry value:

- Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\SmartLine Vision
- Value: EncryptTempFiles=dword:00000001

Applicable values are 1=Enabled, 0=Disabled. The default value is 0.

### Save

If you need to save data from a selected record to your local computer, use **Save** from the shortcut menu or click  on the toolbar.

Use CTRL and/or SHIFT to select and save the data from several records simultaneously.

In case the record has no associated data (its size is 0 or it was not logged), **Save** is disabled in the shortcut menu and on the toolbar.

When you are saving a large file, the following message appears: "Saving file <file path and name>." The message box contains a progress bar. You can click **Cancel** at any time to abort the saving process. In this case the resultant file on the local computer will be incomplete and will contain only that part of the data which was received before you aborted the saving process.

If the data was transferred by the user as a file, it is stored in the shadow log as a file and can be saved to the local computer as a file too.

When a user has written data to a CD/DVD/BD disk, all data is stored in a shadow log as a single CD/DVD/BD image (one image per each written CD/DVD/BD disk or session) in the CUE format.

CD/DVD/BD images as well as other data that originally was not transferred as files (direct media access or serial/parallel ports transfer) have auto-generated names based on the action's type, drive's letter or device's name and time/date (for example, `direct_write(E:) 19:18:29 17.07.2006.bin`).

Each CD/DVD/BD image is saved to the local computer as two files: the data file with the .bin extension (for example, `direct_write(E_) 19_18_29 17_07_2006.bin`) and the cue sheet file that has the same name as its data file with the .cue extension (for example, `direct_write(E_) 19_18_29 17_07_2006_bin.cue`). These both files are necessary to open the CD/DVD/BD image in the external application that supports the CUE format (such as Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO and many others).

### ***Save As Raw Data***

When you select a record that contains the data originally written as an additional session to a multi-session CD/DVD/BD disk, the **Save As Raw Data** item is available in the shortcut menu. It allows you to save the data to the local computer as is (without fixing references to the data in previous sessions).


If you are using the regular saving function (the **Save** command or the toolbar's button), DeviceLock Management Console detects that the CD/DVD/BD image contains a session that refers to the data in other (previous) sessions. Since the previous sessions are not available (they could be written on the computer where DeviceLock Service is not installed), DeviceLock Management Console locates and fixes all references to these non-existent sessions to make the .cue file readable by applications that support this format.

However, if you need to get the data that was not modified by DeviceLock Management Console, use **Save As Raw Data**. In this case the resultant file may be unreadable by applications that support the CUE format.

When saving large files, you can click the **Cancel** button on the progress bar to abort the saving process. In this case the resultant file on the local computer will contain only that part of the data which was received before you aborted the saving process.

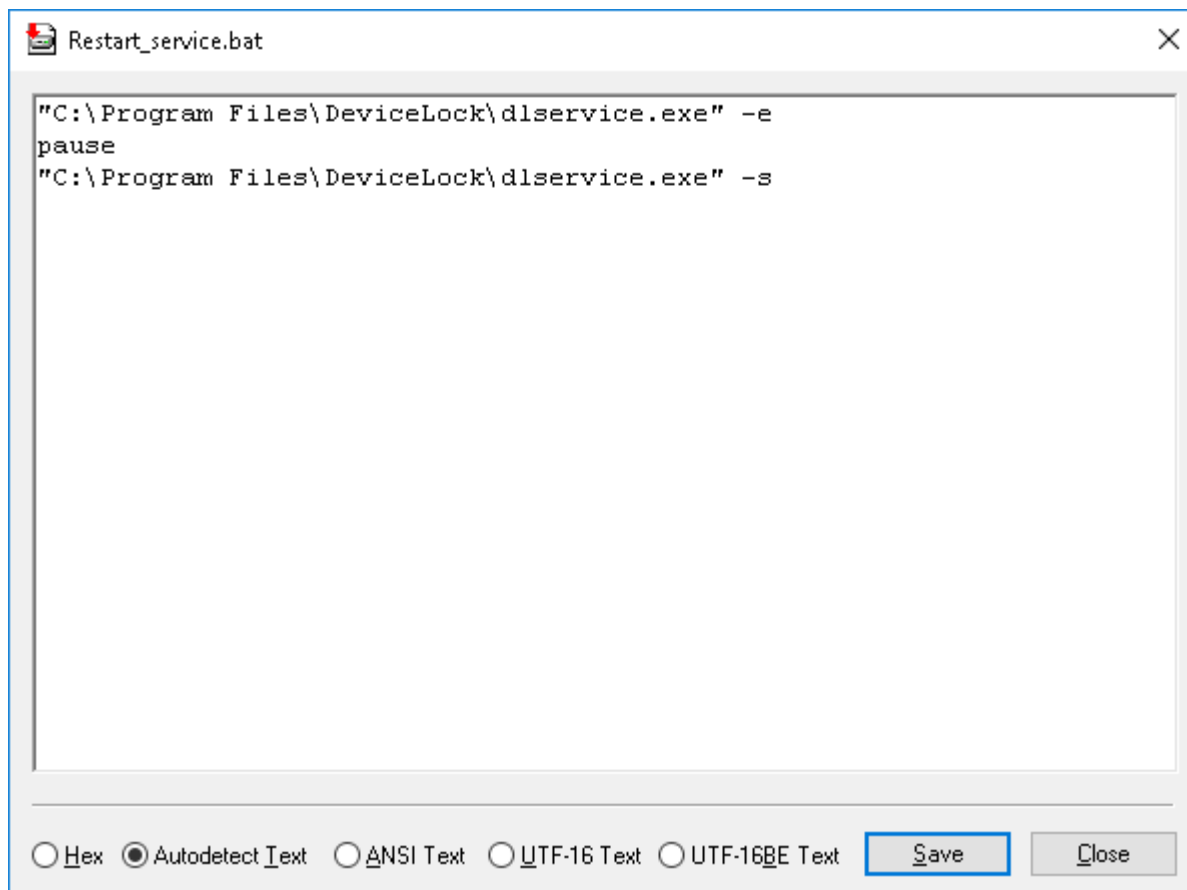
### ***Delete***



To delete a record, select **Delete** from the shortcut menu or click  on the toolbar. Use CTRL and/or SHIFT to select and remove several records simultaneously.

### View

To open the data in the built-in viewer, use **View** from the shortcut menu.



In the built-in viewer, click any of the following viewing options:

- **Hex** - Displays data in hex as well as in words.
- **Autodetect Text** - Auto-detects the text encoding and displays data in text format only.
- **ANSI Text** - Specifies ANSI encoding for text and displays data in text format only.
- **UTF-16 Text** - Specifies Unicode UTF-16 encoding for text and displays data in text format only.
- **UTF-16BE Text** - Specifies Unicode UTF-16 (Big Endian) encoding for text and displays data in text format only.

By clicking **Save** you can save the data from the viewer to an external file.

---

### Note

When opening a large file, you can click **Cancel** on the progress bar to abort the process of opening the file. In this case the viewer shows only the data received before opening the file was aborted.

---

### External Viewer

Also, you can define the external program that will be used to view the shadow data.

If such an external application is defined, the command **External Viewer** is available on the shortcut menu. To define it, add the following registry value on the computer running DeviceLock Management Console:

- Key: HKEY\_CURRENT\_USER\Software\SmartLine Vision\DLManager\Manager
- Value: ExternalShadowViewer=REG\_SZ:<full\_path\_to\_viewer> %1

Here <full\_path\_to\_viewer> must be replaced with the full path to the external application. If the path contains spaces, enclose it in quotation marks. Example:

"C:\Program Files\Microsoft Office\OFFICE11\winword.exe" %1.

---

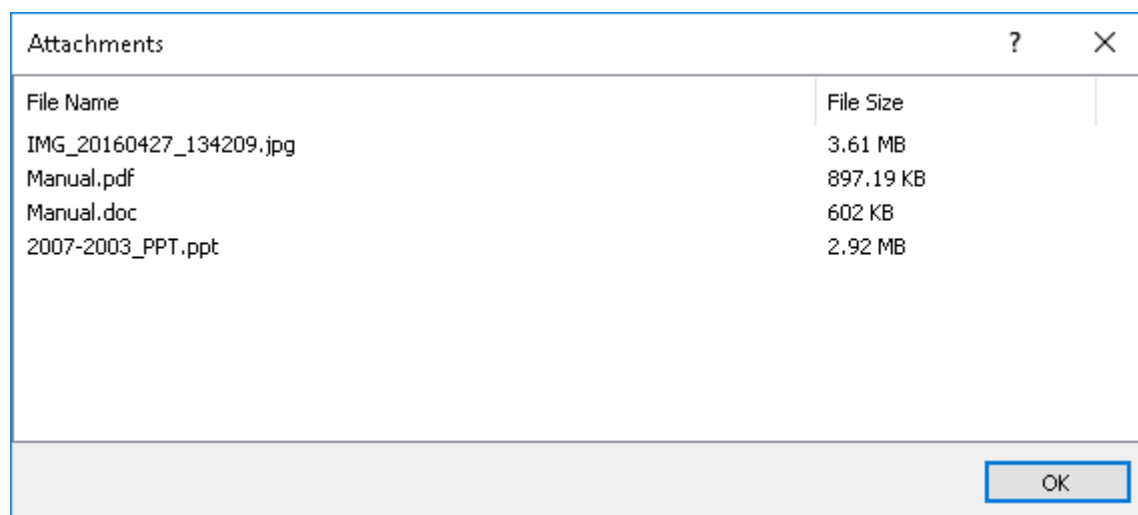
### Note

When opening a large file, you can click **Cancel** on the progress bar to abort the process of opening the file. In this case the application displays only the data received before opening the file was aborted.

---

### View Attachments

The **View Attachments** command lists the attachments (if any) for shadow eml copies of e-mails sent/received via the SMTP, Web Mail, IBM Notes, or MAPI protocol.



The **Attachments** dialog box displays a list of files attached to the selected e-mail message. You can view the following information about each file: the name of the file (with extension) and its size.

You can view attachments by using the Shadow Log Viewer on a client computer, the Shadow Log Viewer on DeviceLock Enterprise Server or the Shadow Log Viewer plug-in of DeviceLock Enterprise Manager.

Administrators of DeviceLock Service and DeviceLock Enterprise Server who do not have access to shadowed data can use the **View Attachments** command to view a list of attachments for shadow copies of e-mail messages.

### View Sender and Recipient(s)







The **View Sender and Recipient(s)** command lists the senders and recipients for shadow copies of messages sent/received via the SMTP, Web Mail, IBM Notes, or MAPI protocol. Administrators of DeviceLock Service and DeviceLock Enterprise Server who do not have access to shadowed data can use this command to find out who and to whom sent a given message.

## Managing the Shadow Log (Service)

The log can be managed by using commands from the shortcut menu:



- In the DeviceLock Management Console tree, expand **DeviceLock Service**, and then right-click **Shadow Log Viewer** under the **DeviceLock Service** node.  
- OR -
- In the DeviceLock Management Console tree, select **DeviceLock Service > Shadow Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Refresh**  - Update the list of records with the latest information.
- **Filter**  - Display only the records that match the conditions specified (see [Shadow Log Filter \(Service\)](#)).
- **Quick filters** - Choose from the following options to display only records for a certain period of time:
  - Current day 
  - Current week 
  - Current month 
  - Current year 


To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

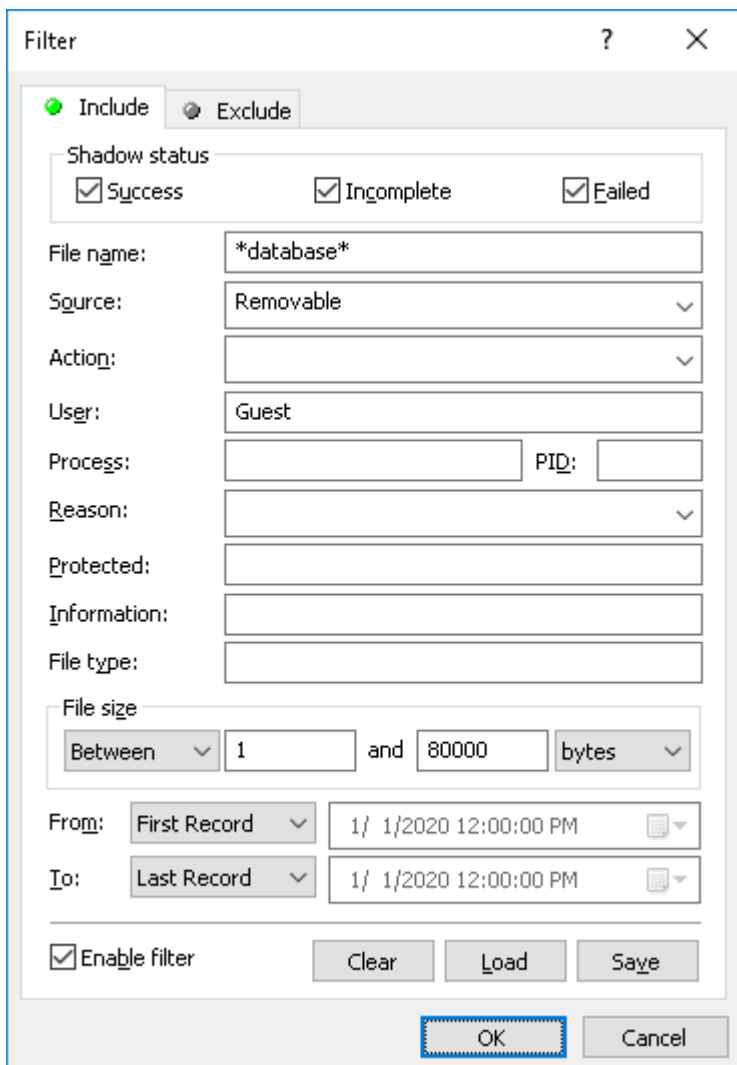
A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Send Data to Server**  - When the [DeviceLock Enterprise Server\(s\)](#) parameter is configured and the **Enable** or **File names only** option is selected for the [Transfer shadow data to server](#) parameter, the **Send Data to Server** command can be used to send log data to the DeviceLock Enterprise Server as soon as possible. Since the server collects log data automatically as it accumulates on the DeviceLock Service, the use of this command is optional.

## Shadow Log Filter (Service)

You can filter data in [Shadow Log Viewer \(Service\)](#) so that only records that meet certain conditions are displayed in the list.

To open the **Filter** dialog box, choose **Filter** from the shortcut menu of **Shadow Log Viewer** or click  on the toolbar.



There is no big difference between defining Audit Log Filter and Shadow Log Filter, so first read the [Audit Log Filter \(Service\)](#) section of this manual.

To set up a filter, select the **Enable filter** check box on the respective tab depending upon whether to configure include or exclude conditions.

---

#### Note

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

When the filter is enabled, you can define its condition by entering values into the following fields:

- **Success** - Specifies whether to filter the successfully logged data.
- **Incomplete** - Specifies whether to filter the data that was logged incompletely.
- **Failed** - Specifies whether to filter the logged data checked by Content-Aware Rules and whose transmission was blocked.

- **File name** - The text that matches a value in the Shadow Log Viewer's **File Name** column. This field is case-insensitive.
- **Source** - The text that matches a value in the Shadow Log Viewer's **Source** column. This field is case-insensitive.
- **Action** - The text that matches a value in the Shadow Log Viewer's **Action** column. This field is case-insensitive.
- **User** - The text that matches a value in the Shadow Log Viewer's **User** column. This field is case-insensitive.
- **Process** - The text that matches a value in the Shadow Log Viewer's **Process** column. This field is case-insensitive.
- **PID** - The number that matches a value in the Shadow Log Viewer's **PID** column. To enter multiple numbers, separate them with a semicolon (;).
- **Reason** - The text that matches a value in the Shadow Log Viewer's **Reason** column. This field is case-insensitive.
- **Protected** - The text that matches a value in the Shadow Log Viewer's **Protected** column.
- **Information** - The text that matches a value in the Shadow Log Viewer's **Information** column. This field is case-insensitive.
- **File type** - The text that matches a value in the Shadow Log's Viewer **File Type** column. This field is case-insensitive.
- **File size** - The number or the range of numbers that matches a value in the Shadow Log Viewer's **File Size** column.
- **From** - The beginning of the range of records to filter. Select **First Record** to filter records from the earliest one in the log. Select **Records On** to filter records made no earlier than a specific date and time.
- **To** - The end of the range of records to filter. Select **Last Record** to filter records up to the latest one in the log. Select **Records On** to filter records made no later than a specific date and time.

---

#### Note

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.

- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

## Managing DeviceLock Service for Mac

DeviceLock Service for Mac can be managed via DeviceLock Management Console in much the same way as you manage DeviceLock Service for Windows (see [Managing DeviceLock Service for Windows](#)).

---

### Note

To allow remote management via DeviceLock management consoles using local user credentials for machine where DeviceLock Service for Mac was installed, the **Share File and Folders using SMB (Windows)** system option must be enabled for these local users or the NTLM hashes must be enabled for these accounts. For more information on this, see [Enabling NTLM authentication for local users on Mac OS X](#).

---

In comparison to DeviceLock Service for Windows, DeviceLock Service for Mac supports only these settings and parameters:

### **Service Options**

- DeviceLock Administrators (unsupported parameters: Enable Unhook Protection, Prevent Changes in System Configuration Files, Use Strong Integrity Check)
- DeviceLock Enterprise Server(s)
- DeviceLock Certificate
- Use Group/Server Policy
- Fast servers first
- Offline mode detection
- Override Local Policy
- Log policy changes and Start/Stop events

### **Service Options > Auditing & Shadowing**

- Transfer shadow data to server

### **Service Options > Encryption**

- Mac OS X FileVault

### **Devices**

- Bluetooth (Permissions, Audit)
- FireWire port (Permissions, Audit)
- Hard disk (Permissions, Audit)
- Optical Drive (Permissions, Audit)

- Removable (Permissions, Audit, Shadowing)
- Serial port (Permissions, Audit)
- USB port (Permissions, Audit)
- WiFi (Permissions, Audit)
- USB White List (the only flag supported is Control as type)
- Media White List

---

**Note**

Bluetooth permissions are not applied to Bluetooth HID devices, so access to the devices is always allowed to prevent wireless HID devices (mice and keyboards) from being disabled on iMac and Mac Pro hardware.

---

**Security Settings**

- Access control for USB HID
- Access control for USB Bluetooth adapters
- Access control for USB and FireWire network cards
- Access control for USB storage devices
- Access control for FireWire storage devices

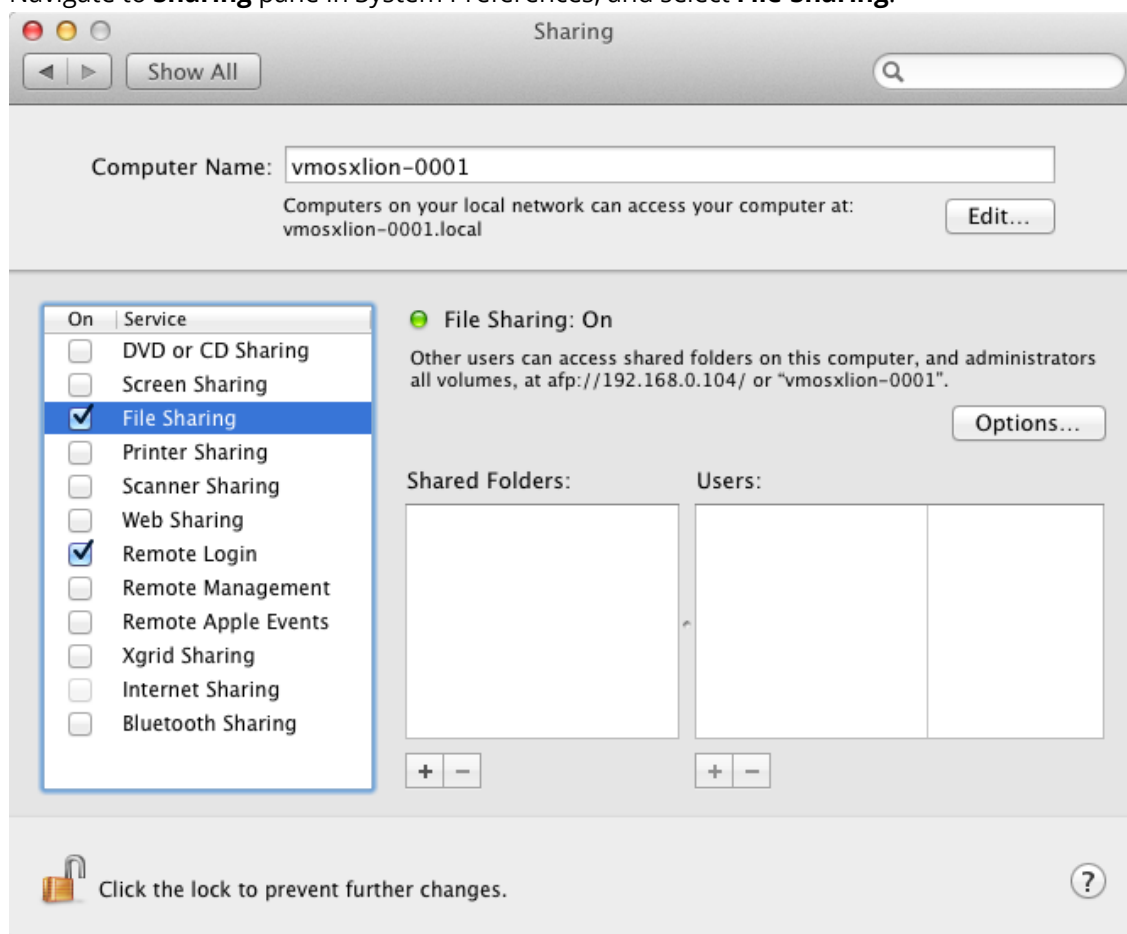
## Enabling NTLM authentication for local users on Mac OS X

The DeviceLock Service for Mac employs NTLM authentication and encryption in order to secure network communications with other DeviceLock components. If the Mac computer is integrated in Active Directory authentication with a domain account, it will just work. However, NTLM authentication with local users is normally disabled. In order to manage a standalone Mac with DeviceLock management consoles, NTLM authentication **MUST** be enabled for the local user.

There are two ways to enable NTLM for a local user on Mac:

1. **The user-friendly way.** This method works for Mac OS X 10.7 and later. See below for the 10.6 method.

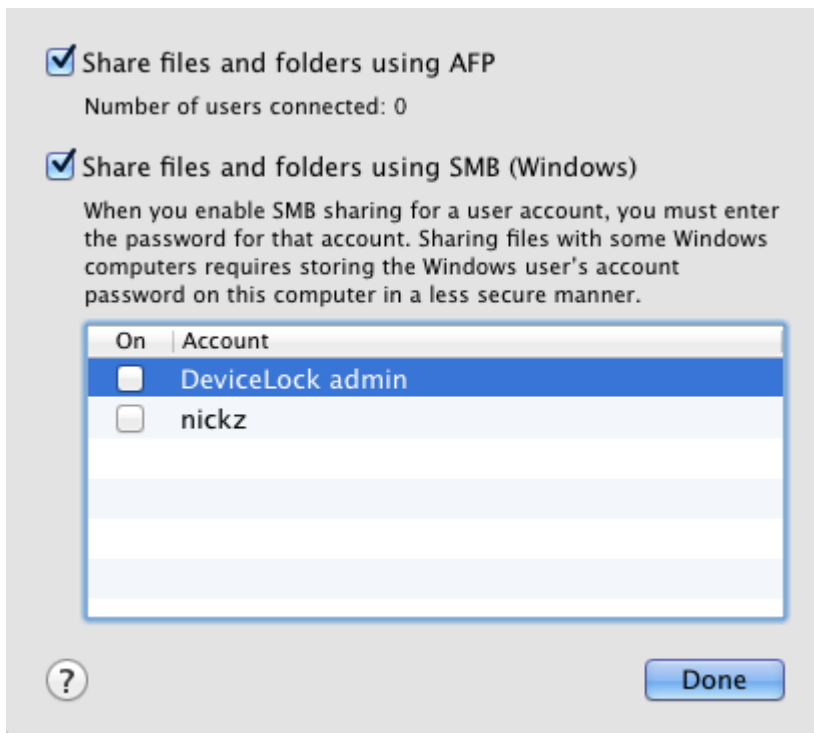
- a. Navigate to **Sharing** pane in System Preferences, and select **File Sharing**.



- b. Click **Options**.

The dialog box that appears provides a list of local users. Selecting the **Share files and folder using SMB** check box turns on the support for NTLM authentication for each user selected in that list.

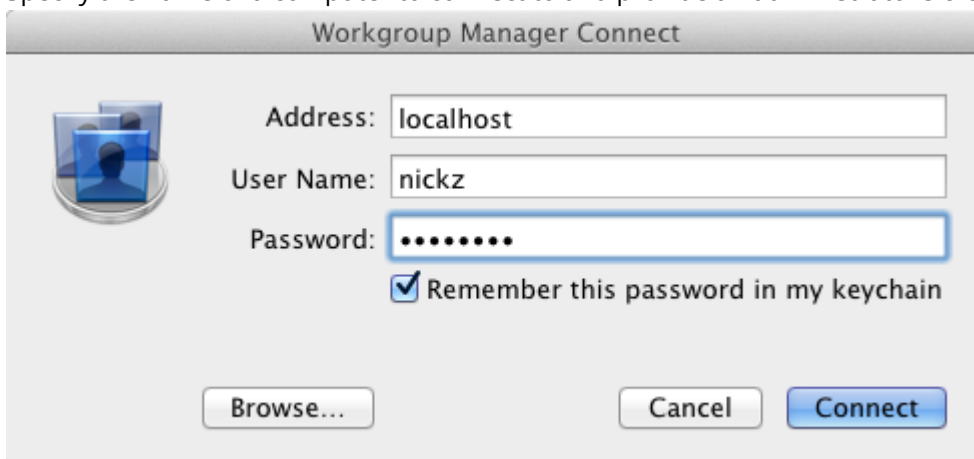




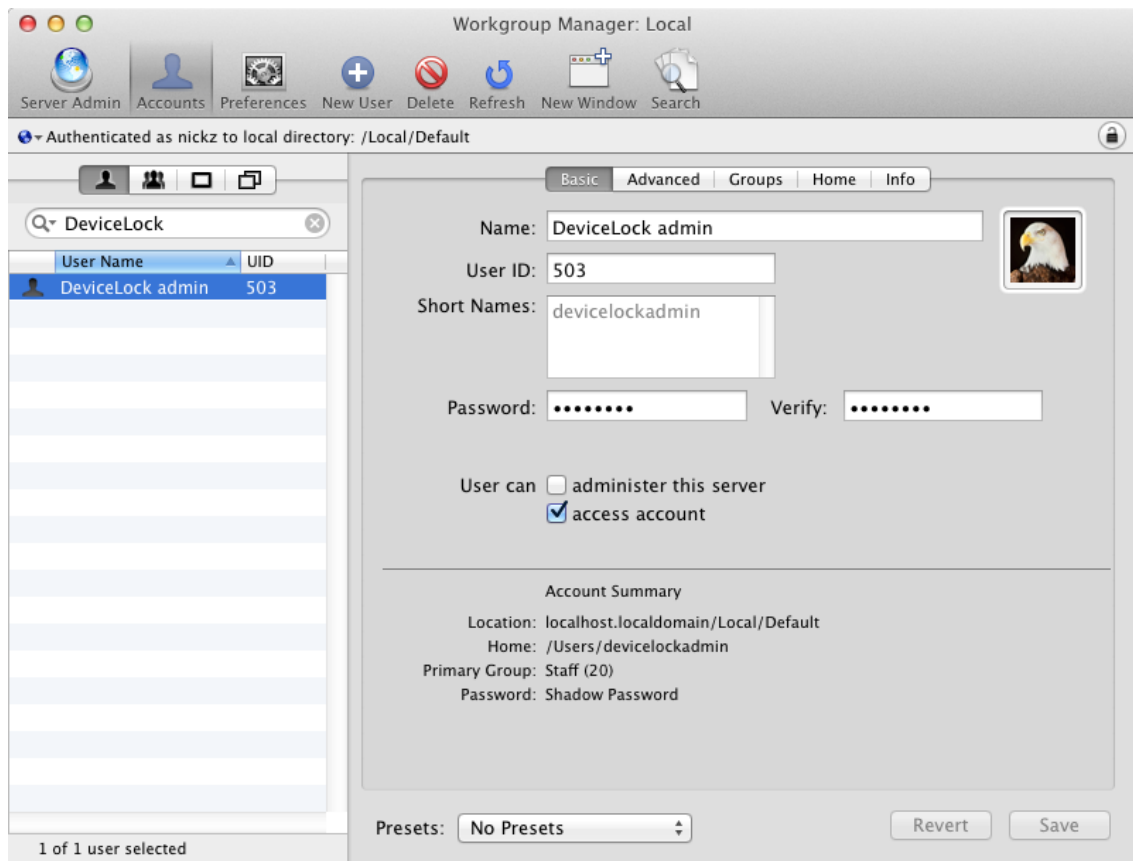
#### Note

The support for NTLM authentication is enabled on a per-user basis.

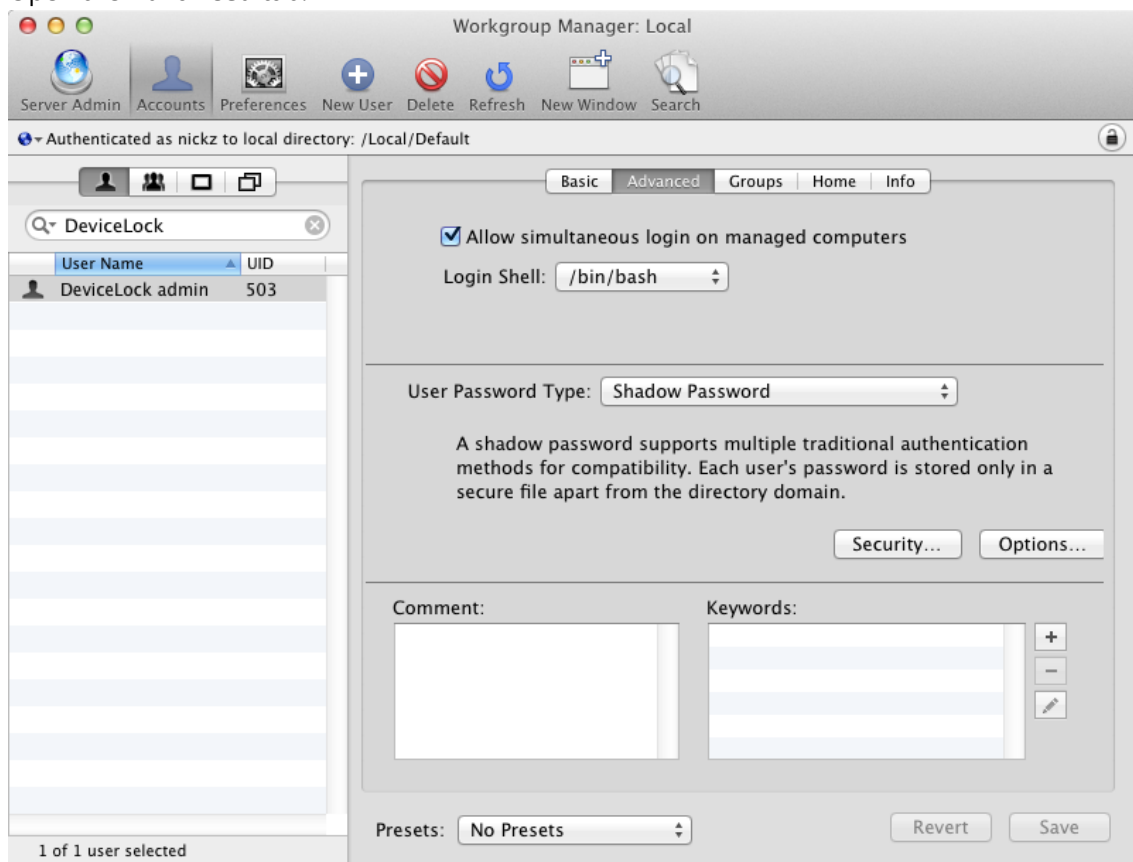
2. **The alternate way.** This method works for Mac OS X 10.6, 10.7 and later.
  - a. Install Server Admin Tools:
    - Server Admin Tools 10.6.8 <http://support.apple.com/kb/HT3931>
    - Server Admin Tools 10.7.3 <http://support.apple.com/kb/HT202366>
  - b. Launch Workgroup Manager from Server Admin Tools. The authentication dialog will pop up. Specify the name of a computer to connect to and provide an administrator's credentials.



- c. After successful authentication, the main window appears. Select a user from the list to the left.



d. Open the **Advanced** tab.



- e. Click the **Security** button.
- f. In the dialog box that appears, select the **NTLMv1 and NTLMv2** check box, and apply changes. Then, change the password of the user for which you have enabled the NTLM authentication.



---

**Note**

- NTLM authentication will not be available until the user password is changed. This is the inherent limitation of the secure password database of Mac OS X. The new password is not required to be different from the old one.
  - The support for NTLM authentication is enabled on a per-user basis.
-

# Content-Aware Rules (Regular Profile)

## Rules for Devices

Content-Aware Rules extend the basic port/device contextual access control functionality of the DeviceLock DLP by adding comprehensive content-level protection of corporate documents containing confidential company information. They enable automatic content inspection of data copied to external storage devices, detection of sensitive content, and help with enforcement of regulatory policies.

Content-Aware Rules can selectively allow or deny access to specific file content regardless of preset permissions at the device type-level. They can also be used to allow or deny the shadow copying of specific content, or to just detect attempts to read, write or delete specific content without necessarily blocking access or creating shadow copies. For flexibility, Content-Aware Rules can be defined per device channel on a per-user or per-group basis.

It is possible to apply Content-Aware Rules to access control operations, to shadow copy operations, to detection operations, or configure them to perform all of the above.

The following examples illustrate the use of Content-Aware Rules.

- **Example 1 - Using Content-Aware Rules for access control operations.** Rules can be configured to allow certain users or groups to read files specifically containing a phrase like “not for distribution” from Removable, Floppy and Optical devices, but still prevent them from writing files containing sensitive data to the same Removable, Floppy and Optical devices.
- **Example 2 - Using Content-Aware Rules for shadow copy operations.** Rules can be configured so that just files containing identifiable patterns like credit card numbers, Social Security numbers, bank routing numbers, or even just key words like “Secret”, “Confidential”, “Restricted,” or the phrases “Top Secret”, and “For Official Use Only” will be shadow copied for security auditing and incident investigation purposes.
- **Example 3 - Using Content-Aware Rules for unusual event detection operations.** Rules can be configured so that only attempts to transfer files exceeding 20 MB, for example, will be audit logged and alerted on, without necessarily blocking/delaying the actual transfer or creating shadow copies.

Content-Aware Rules can be applied in various ways to the following device types: Clipboard, Floppy, iPhone, MTP, Optical Drive, Palm, Printer, Removable, TS Devices, and Windows Mobile.

---

## Note

When defining Content-Aware Rules for the Printer device type, consider the following:

- DeviceLock Service can perform content analysis of documents sent to print, but only if the following options are selected on the **Advanced** tab of the printer's **Properties** dialog box: **Spool print documents so program finishes printing faster** and **Start printing after last page is spooled**.
  - File Type Detection content groups and the following parameters of Document Properties and Digital Fingerprints content groups are not applicable to documents sent to print: **File size, Modified, File name, Accessed by process, Password protected, Contains text, Additional parameters, Exact file match, Use only binary fingerprints for password protected documents**.
- 

## Content-Aware Rules Node

Under the **Devices > Content-Aware Rules** node in the console tree, the console displays a list of users and groups that have content-aware rules specified for devices. Content-aware rules can be specified individually for every user and group per device type channel.

---

## Note

Different online vs. offline Content-Aware Rules can be defined for the same user or groups of users. Online Content-Aware Rules (Regular Profile) apply to client computers that are working online. Offline Content-Aware Rules (Offline Profile) apply to client computers that are working offline based upon status of the Offline Detection Mode used. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define offline Content-Aware Rules, see [Managing Offline Content-Aware Rules for Devices](#).

---

The shortcut menu of the **Content-Aware Rules** node provides the following commands:

- **Manage** - Opens a dialog box to view, set, or change the online (regular) content-aware rules.
- **Manage Offline** - Opens a dialog box to view, set, or change the offline content-aware rules.
- **Load** - Loads a previously saved regular content-aware rules template from an external file.
- **Load Offline** - Loads a previously saved offline content-aware rules template from an external file.
- **Save** - Saves the regular content-aware rules to an external template file.
- **Save Offline** - Saves the offline content-aware rules to an external template file.
- **Undefine** - Resets the regular content-aware rules to the "unconfigured" state. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Undefine Offline** - Resets the offline content-aware rules to the "unconfigured" state. If the offline content-aware rules are undefined, the regular rules are applied to offline client computers.

- **Remove Offline** - Blocks the inheritance of the offline content-aware rules and enforces the regular rules. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).

Users or groups to which content-aware rules apply are displayed under the **Content-Aware Rules** node in the console tree and have the same shortcut menu as that node, with the exceptions of the **Undefine Offline** command and the **Delete User** command (which deletes the content-aware rules for the selected user or group).

For further details, see:

[Configuring Content Groups](#)

[Managing Content-Aware Rules](#)

## List of Content-Aware Rules for Devices

The users and groups that have content-aware rules specified for devices are displayed under the **Devices > Content-Aware Rules** node in the console tree (see [Content-Aware Rules Node](#)).

When a user or group is selected under the **Content-Aware Rules** node in the console tree, the details pane lists the content-aware rules specified for that user or group. For each rule, the list provides the following details:

- **Name** - The name of the rule. By default, the rule has the same name as its content group.
- **Type** - The type of the content analysis. Possible values:
  - **File Type Detection** - Recognition and identification of a file's true file type are based on its actual characteristic signatures found by inspection rather than just its name.
  - **Keywords** - Recognition and identification of data/files are based on the specified keywords or phrases found by inspection.
  - **Pattern** - Recognition and identification of data/files is based on the specified patterns of alphanumeric text described by Perl regular expressions and found by inspection.
  - **Document Properties** - Recognition and identification of files are based on their basic file properties (i.e. size, name, header information, date modified, etc.).
  - **Digital Fingerprints** - Recognition and identification of files are based on their digital fingerprints.
  - **Complex** - Recognition and identification of data/files are based on the content described by a Boolean expression of multiple rule types.
- **Action(s)** - Shows which user actions are allowed or disallowed on files and which user actions are logged to the Shadow Log.
- **Applies To** - Possible values:
  - **Permissions** - The rule applies to access control operations.
  - **Shadowing** - The rule applies to shadow copy operations.
  - **Detection** - The rule applies to detection operations.

- **Permissions+Shadowing** - The rule applies to both access control and shadow copy operations.
- **Permissions+Detection** - The rule applies to both access control and detection operations.
- **Shadowing+Detection** - The rule applies to both shadow copy and detection operations.
- **Permissions+Shadowing+Detection** - The rule applies to all available operations: access control, shadow copy and detection.
- **Device Type(s)** - The device type(s) to which the rule applies.
- **Send Alert** - Shows whether alerts are enabled or disabled for this rule.
- **Log Event** - Shows whether the audit logging of events associated with this rule is enabled or disabled.
- **Shadow Copy** - Shows whether the shadow copying is enabled or disabled for this rule.
- **Profile** - Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to computers that are working offline.  
Different online vs. offline Content-Aware Rules can be defined for the same user(s) or groups of users. For information about how to define offline Content-Aware Rules, see [Managing Offline Content-Aware Rules for Devices](#).

The shortcut menu on a rule in the details pane provides the following commands:

- **Manage** - Depending on the rule's profile (regular or offline), opens a dialog box to define the online (regular) or offline content-aware rules.
- **Edit** - Opens a dialog box to view or modify the rule.
- **Send Alert** - Enables or disables alerts for the given rule.
- **Log Event** - Enables or disables the audit logging of events associated with the given rule.
- **Shadow Copy** - Enables or disables the shadow copying of the content that causes the rule to trigger.
- **Delete** - Deletes the given rule.

For further details, see [Managing Content-Aware Rules](#).

## Access Control

When Content-Aware Rules apply to access control operations, they control read, write and delete operations for specified content. No separate rules can be configured for delete operations. Delete and write operations are controlled together by the Write access right.

By using Content-Aware Rules for devices, one can do the following:

- Grant read/write access to specified file content when access is denied at the device type-level.
- Deny read/write access to specified file content when access is granted at the device type-level.

---

**Note**

DeviceLock can check access to devices at two levels: the interface (port) level and the device type level. Some devices are checked at both levels, while others only at one level - either interface (port) or device type. For example, a USB flash drive belongs to both levels: interface (USB port) and device type (Removable). Content-Aware Rules work only when access checking occurs at the device type level (Removable, Floppy, etc.). DeviceLock does not perform the access check for USB devices at the device type level if the following conditions are true:

- The device is not added to the USB Devices White List, **Access control for USB storage devices** is enabled in **Security Settings**, and the user has no access by user, group, or built-in context membership in the ACL for **USB port**.  
- OR -
  - The device is added to the USB Devices White List and the **Control As Type** check box is not selected for the white list device assignment.
- 

The following table provides summary information on access rights that can be specified in Content-Aware Rules.

Access rights	Description
Generic: Read	Controls whether the user can read files with specified content from a device. Applies to Optical Drive, Floppy and Removable devices.
Generic: Write	Controls whether the user can write files with specified content to a device. Applies to Floppy and Removable devices.
Generic: Read, Write	Controls whether the user can read and write files with specified content from and to a device. Applies to Floppy and Removable devices.
Generic: Print	Controls whether the user can print documents with specified content. Applies only to the Printer device type.
Generic: Mapped Drives Read	Controls whether the user can read data with specified content from a mapped drive during a terminal session. Applies only to TS Devices.
Generic: Mapped Drives Write	Controls whether the user can write data with specified content to a mapped drive during a terminal session. Applies only to TS Devices.
Generic: Clipboard Incoming Text	Controls whether the user can paste text data with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming File	Controls whether the user can paste files with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming Image	Controls whether the user can paste images with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming Unidentified Content	Controls whether the user can paste any other uncategorized data with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.



Generic: Clipboard Outgoing Text	Controls whether the user can paste text data with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing File	Controls whether the user can paste files with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Image	Controls whether the user can paste images with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Unidentified Content	Controls whether the user can paste any other uncategorized data with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Encrypted: Read	Controls whether the user can read files with specified content from a DeviceLock-verified encrypted device. Applies only to Removable devices.
Encrypted: Write	Controls whether the user can write files with specified content to a DeviceLock-verified encrypted device. Applies only to Removable devices.
Encrypted: Read, Write	Controls whether the user can read and write files with specified content from and to a DeviceLock-verified encrypted device. Applies only to Removable devices.
Special Permissions: Copy Text	Controls whether the user can paste text data with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy Unidentified Content	Controls whether the user can paste any other uncategorized data with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy File	Controls whether the user can paste files with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy Image	Controls whether the user can paste images with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Screenshot	Controls whether the user can paste screenshots with specified content from the clipboard. Applies only to the Clipboard device type.

## Note

Generic access rights specified for Removable devices apply only to unencrypted devices. Encrypted access rights specified for Removable devices apply only to encrypted devices. To specify access rights for both encrypted and unencrypted Removable devices, both Generic and Encrypted access rights must be specified. For a list of devices that DeviceLock Service recognizes as encrypted, see [Encryption](#).

The following table shows how different device type-level and file-level permissions affect the user permission state. Device type-level permissions are permissions set for a device type. File-level permissions are permissions defined by Content-Aware Rules.

Full Access device type-level	No Access device type-level	Allow ReadDeny Write device type-level
----------------------------------	--------------------------------	---

<b>Allow Read</b> file-level	Allows read access to all content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies read access to all but specified content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.	Allows read access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Deny Read</b> file-level	Denies read access to specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies read and write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies read access to specified content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Allow Write</b> file-level	Allows write access to all content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies write access to all but specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies write access to all but specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Deny Write</b> file-level	Denies write access to specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies read and write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Allow Read</b> <b>Allow Write</b> file level	Allows read and write access to all content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies read and write access to all but specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Allows read access to all content. Denies write access to all but specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Deny Read</b> <b>Deny Write</b> file-level	Denies read and write access to specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies read and write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies read access to specified content. Denies write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Allow Read</b> <b>Deny Write</b> file-level	Allows read access to all content. Denies write access to specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies read access to all but specified content. Denies write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.	Allows read access to all content. Denies write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Deny Read</b> <b>Allow Write</b>	Denies read access to specified content. Allows write access to all content.	Denies read access to all content. Denies write access to all but specified content.	Denies read access to specified content. Denies write access to all but

file-level	Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	specified content. Allows creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Shadowing:</b>	Allows read and write access to all content.	Denies read and write access to all content.	Allows read access to all content.
<b>Allow / Deny</b>	Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.
file-level			
<b>Detection:</b>	Allows read and write access to all content.	Denies read and write access to all content.	Allows read access to all content.
<b>Allow Read /</b>	Allows creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies creation, deletion, and renaming of empty folders and zero byte (0) files.	Denies write access to all content. Denies creation, deletion, and renaming of empty folders and zero byte (0) files.
<b>Allow Write</b>			
file-level			

## Note

If the No Access permission condition is set for a device type and there is a Content-Aware Rule that allows write access to certain content, or content detection for the same device type for specified users/groups, the Traverse Folder permission is granted to these users/groups for this device type. The Traverse Folder permission allows the user to move through folders and see files and folders located in subdirectories even if the user has no Read permission for the traversed folders.

When using Content-Aware Rules, consider the following:

- Content-Aware Rules with **Deny** settings take priority over rules with **Allow** settings if they apply to the same users or groups (or any of the same group member users) over the same device type.  
Exception: Content-Aware Rules with **Allow** settings based on a Document Properties group with the **Text extraction not supported** option selected will take priority over rules with **Deny** settings and will allow transfer of any matching content, including split (or multi-volume) archives.  
Exception: An **Allow** Content-Aware Rule based on a Document Properties group with the **Password protected** option selected takes priority over **Deny** rules (if any) and allows transfer of any matching content. A Complex **Allow** Content-Aware Rule Boolean will take priority only if there is a Document Properties group with the **Password protected** option selected among a set of logically connected content groups that the file matched.  
Exception: An **Allow** Content-Aware Rule based on a Digital Fingerprints group with the **Exact file match** option selected takes priority over **Deny** rules (if any) and allows transfer of any matching content. A Complex **Allow** Content-Aware Rule Boolean will take priority only if there is a Digital Fingerprints group with the **Exact file match** option selected among a set of logically connected content groups that the file matched.

- Content-Aware Rules with **Allow** settings will allow transfer of the whole data object (message or file, including archives and other containers) when the content matches these rules and when the content does not match a Content-Aware Rule with **Deny** settings.
- To prevent the deletion of the original file when users try to overwrite the existing file with a new file to which they are denied write access, enable the [Safe file overwrite](#) parameter in [Service Options](#).
- To prevent the deletion of the original file when users try to modify a file to which they are denied write access, enable the [Safe file overwrite](#) parameter in [Service Options](#).
- To prevent the deletion of the original file when users open the file, modify it by inserting the content to which they are denied write access, and then try to save changes, enable the [Safe file overwrite](#) parameter in [Service Options](#).
- Unsafe removal of a device can result in the corruption of the device's file system and data.
- When users try to copy files to which they are denied write access, these files appear to be temporarily visible in Windows Explorer or other file manager applications. In actuality, these files do not really exist on the target device, but they are located in the memory cache and are removed from this cache immediately after DeviceLock finishes checking their content.
- Checking the content of files can be a time-consuming operation. The device cannot be safely removed while this operation is in progress, even if the copied files become visible in Windows Explorer or other file manager applications. In this situation, the user receives an error message indicating that the device is currently busy.
- Newly copied files cannot be opened for reading until DeviceLock finishes checking their content.
- Checking the content of files can be a time-consuming operation. The DeviceLock administrator can define a content verification message to be displayed to users when content inspection is in progress. For detailed information on this message, see the [Content verification message](#) parameter description in [Service Options](#).
- When users try to read or write files to which they are denied read or write access, they will be displayed a content-aware blocked read or write message if the respective message is enabled in Service Options. For detailed information on these messages, see description of the [Content-Aware blocked read message](#) and [Content-Aware blocked write message](#) parameters in [Service Options](#).

## Content-Aware Shadowing

Before Content-Aware Rules can be used for shadow copy operations, one must turn on shadowing in **Auditing, Shadowing and Alerts** at the device type-level. Content-Aware Rules that apply to shadow copy operations will filter the shadow copies of data and files written by the user. As compared to shadowing purely by device type channel, this feature can significantly reduce the amount of triggered shadowed files to just those that contain sensitive or at least interesting data that can be looked at further by the audit team.

The following table provides summary information on shadowing rights that can be specified in Content-Aware Rules.

Shadowing rights	Description
Generic: Read	Controls whether to create shadow copy of data with specified content read from a device. Applies only to the MTP device type.
Generic: Write	Controls whether to create shadow copy of data with specified content written to a device. Applies to Floppy, iPhone, MTP, Removable, Palm and Windows Mobile devices.
Generic: Mapped Drives Write	Controls whether to create shadow copy of data with specified content written to a device. Applies only to TS Devices.
Generic: Print	Controls whether to create shadow copy of documents with specified content sent to printers. Applies only to the Printer device type.
Generic: Copy to clipboard	Controls whether to create shadow copy of data with specified content pasted from the clipboard. Applies only to the Clipboard device type.
Generic: Clipboard Incoming Text	Controls whether to create shadow copy of text data with specified content pasted from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Text	Controls whether to create shadow copy of text data with specified content pasted from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming Image	Controls whether to create shadow copy of images with specified content pasted from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Image	Controls whether to create shadow copy of images with specified content pasted from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming File	Controls whether to create shadow copy of files with specified content pasted from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing File	Controls whether to create shadow copy of files with specified content pasted from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming Unidentified Content	Controls whether to create shadow copy of any uncategorized data with specified content pasted from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic:	Controls whether to create shadow copy of any uncategorized data with specified

Clipboard Outgoing Unidentified Content	content pasted from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Encrypted: Write	Controls whether to create shadow copy of data with specified content written to an encrypted device. Applies only to Removable devices.
Special Permissions: Write Calendar	Controls whether to create shadow copy of data with specified content written to a calendar on a mobile device from a PC. Applies to iPhone, Palm and Windows Mobile devices.
Special Permissions: Write Contact	Controls whether to create shadow copy of contacts with specified content written from a PC to a mobile device. Applies to iPhone, Palm and Windows Mobile devices.
Special Permissions: Write E-mail	Controls whether to create shadow copy of email messages with specified content written from a PC to a mobile device. Applies to iPhone, Palm and Windows Mobile devices. For iPhone, this right controls the shadow copying of email account settings but not email messages because iTunes does not support sync of messages.
Special Permissions: Write Attachment	Controls whether to create shadow copy of email attachments with specified content written from a PC to a Windows Mobile or Palm device.
Special Permissions: Write Favorite	Controls whether to create shadow copy of favorites with specified content written from a PC to a Windows Mobile or iPhone device.
Special Permissions: Write File	Controls whether to create shadow copy of files with specified content written from a PC to a mobile device. Applies to iPhone, Palm and Windows Mobile devices.
Special Permissions: Write Media	Controls whether to create shadow copy of media data with specified content written using Windows Media Player to a Windows Mobile device from a PC and media files with specified content written to a Palm or iPhone device from a PC.
Special Permissions: Write Backup	Controls whether to create shadow copy of the iPhone backup data with specified content written from a PC to iPhone.
Special Permissions: Write Note	Controls whether to create shadow copy of notes with specified content written from a PC to a mobile device. Applies to iPhone, Palm and Windows Mobile devices.
Special Permissions: Write Pocket Access	Controls whether to create shadow copy of Pocket Access databases with specified content written from a PC to a Windows Mobile device.
Special	Controls whether to create shadow copy of tasks with specified content written from a PC

Permissions: Write Task	to a mobile device. Applies to Palm and Windows Mobile devices.
Special Permissions: Write Expense	Controls whether to create shadow copy of Palm Expense application data with specified content written from a PC to a Palm device.
Special Permissions: Write Document	Controls whether to create shadow copy of Palm documents with specified content written from a PC to a Palm device.
Special Permissions: Write Unidentified Content	Controls whether to create shadow copy of any uncategorized data with specified content written from a PC to a Windows Mobile device.
Special Permissions: Copy Text	Controls whether to create shadow copy of text data with specified content pasted from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy File	Controls whether to create shadow copy of files with specified content pasted from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy Image	Controls whether to create shadow copy of images with specified content pasted from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Screenshot	Controls whether to create shadow copy of screenshots with specified content pasted from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy Unidentified Content	Controls whether to create shadow copy of any uncategorized data with specified content pasted from the clipboard. Applies only to the Clipboard device type.

---

#### Note

**Generic** shadowing rights specified for the **Removable device** type apply only to unencrypted devices. **Encrypted** shadowing rights specified for the **Removable device** type apply only to encrypted devices. To specify shadowing rights for both encrypted and unencrypted Removable devices, one must specify both **Generic** and **Encrypted** shadowing rights.

---

## Content-Aware Detection

When Content-Aware Rules apply to detection operations, they detect read, write, and delete attempts for specified content for the purposes of auditing and/or alerting rather than for blocking

access and/or shadowing. No separate rules can be configured for delete operations. Delete and write operations are controlled together by the Write access right.

The following table provides summary information on detection rights that can be specified in Content-Aware Rules.

Detection rights	Description
Generic: Read	Controls whether to detect user attempts to read data with specified content from a device. Applies only to Optical Drive, Floppy and Removable devices.
Generic: Write	Controls whether to detect user attempts to write data with specified content to a device. Applies only to Floppy and Removable devices.
Generic: Read, Write	Controls whether to detect user attempts to read or write data with specified content from/to a device. Applies to Floppy and Removable devices.
Generic: Copy to clipboard	Controls whether to detect user attempts to paste data with specified content from the clipboard. Applies only to the Clipboard device type.
Generic: Print	Controls whether to detect user attempts to print documents with specified content. Applies only to the Printer device type.
Generic: Mapped Drives Read	Controls whether to detect user attempts to read data with specified content from a mapped drive. Applies only to TS Devices.
Generic: Mapped Drives Write	Controls whether to detect user attempts to write data with specified content to a mapped drive. Applies only to TS Devices.
Generic: Clipboard Incoming Text	Controls whether to detect user attempts to paste text data with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming File	Controls whether to detect user attempts to paste files with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming Image	Controls whether to detect user attempts to paste images with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Incoming Unidentified Content	Controls whether to detect user attempts to paste any uncategorized data with specified content from the clipboard to a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Text	Controls whether to detect user attempts to paste text data with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing File	Controls whether to detect user attempts to paste files with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Generic: Clipboard Outgoing Image	Controls whether to detect user attempts to paste images with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.



Generic: Clipboard Outgoing Unidentified Content	Controls whether to detect user attempts to paste any uncategorized data with specified content from the clipboard from a terminal session/virtual machine. Applies only to TS Devices.
Encrypted: Read	Controls whether to detect user attempts to read data with specified content from an encrypted device. Applies only to Removable devices.
Encrypted: Write	Controls whether to detect user attempts to write data with specified content to an encrypted device. Applies only to Removable devices.
Encrypted: Read, Write	Controls whether to detect user attempts to read or write data with specified content from/to an encrypted device. Applies only to Removable devices.
Special Permissions: Copy Text	Controls whether to detect user attempts to paste text data with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy File	Controls whether to detect user attempts to paste files with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy Image	Controls whether to detect user attempts to paste images with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Screenshot	Controls whether to detect user attempts to paste screenshots with specified content from the clipboard. Applies only to the Clipboard device type.
Special Permissions: Copy Unidentified Content	Controls whether to detect user attempts to paste any uncategorized data with specified content from the clipboard. Applies only to the Clipboard device type.

## Rules for Protocols

Content-Aware Rules extend the protocol contextual access control functionality of DeviceLock DLP by adding comprehensive content-level protection of corporate data containing confidential company information. They enable automatic content inspection of data/files transmitted over the network, detection of sensitive content and help with the enforcement of regulatory policies.

Content-Aware Rules can selectively allow or deny access to specific content transmitted over the network regardless of the preset permissions at the protocol-level. They can also be used to allow or deny the shadow copying of specific content, or to detect user attempts to transfer specific content over a protocol without blocking transfer or creating shadow copies. For flexibility, Content-Aware Rules can be defined per network protocol channel on a per-user or per-group basis.

It is possible to apply Content-Aware Rules to access control operations, to shadow copy operations, to detection operations, or configure them to perform all of the above.

The following examples illustrate the use of Content-Aware Rules.

- **Example 1 - Using Content-Aware Rules for access control operations.** Rules can prevent certain users or groups from uploading files containing credit card numbers, telephone numbers, and addresses to an FTP server.

- **Example 2 - Using Content-Aware Rules for shadow copy operations.** Rules can be configured so that IM conversations containing credit card numbers and/or email addresses will be shadow copied for security auditing and incident investigation purposes.
- **Example 3 - Using Content-Aware Rules for detection operations.** Rules can be configured so that any attempts to transfer executable files will be audit logged and alerted on, without blocking the transfer or creating shadow copies.

## Content-Aware Rules Node

Under the **Protocols > Content-Aware Rules** node in the console tree, the console displays a list of users and groups that have content-aware rules specified for protocols. Content-aware rules can be specified individually for every user and group.

---

### Note

Different online vs. offline Content-Aware Rules can be defined for the same user or groups of users. Online Content-Aware Rules (Regular Profile) apply to client computers that are working online. Offline Content-Aware Rules (Offline Profile) apply to client computers that are working offline based upon status of the Offline Detection Mode used. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define offline Content-Aware Rules for protocols, see [Managing Offline Content-Aware Rules for Protocols](#).

---

The shortcut menu of the **Content-Aware Rules** node provides the following commands:

- **Manage** - Opens a dialog box to view, set, or change the online (regular) content-aware rules.
- **Manage Offline** - Opens a dialog box to view, set, or change the offline content-aware rules.
- **Load** - Loads a previously saved regular content-aware rules template from an external file.
- **Load Offline** - Loads a previously saved offline content-aware rules template from an external file.
- **Save** - Saves the regular content-aware rules to an external template file.
- **Save Offline** - Saves the offline content-aware rules to an external template file.
- **Undefine** - Resets the regular content-aware rules to the “unconfigured” state. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Undefine Offline** - Resets the offline content-aware rules to the “unconfigured” state. If the offline content-aware rules are undefined, the regular rules are applied to offline client computers.
- **Remove Offline** - Blocks the inheritance of the offline content-aware rules and enforces the regular rules. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).

Users or groups to which content-aware rules apply are displayed under the **Content-Aware Rules** node in the console tree and have the same shortcut menu as that node, with the exceptions of the

**Undefine Offline** command and the **Delete User** command (which deletes the content-aware rules for the selected user or group).

For further details, see:

[Configuring Content Groups](#)

[Managing Content-Aware Rules](#)

## List of Content-Aware Rules for Protocols

The users and groups that have content-aware rules specified for protocols are displayed under the **Protocols > Content-Aware Rules** node in the console tree (see [Content-Aware Rules Node](#)).

When a user or group is selected under the **Content-Aware Rules** node in the console tree, the details pane lists the content-aware rules specified for that user or group. For each rule, the list provides the following details:

- **Name** - The name of the rule. By default, the rule has the same name as the content group selected for that rule.
- **Type** - The type of the content analysis. Possible values:
  - **File Type Detection** - Recognition and identification of a file's true file type are based on its actual characteristic signatures found by inspection rather than just its name.
  - **Keywords** - Recognition and identification of data/files are based on the specified keywords or phrases found by inspection.
  - **Pattern** - Recognition and identification of data/files is based on the specified patterns of alphanumeric text described by Perl regular expressions and found by inspection.
  - **Document Properties** - Recognition and identification of files are based on their basic file properties (i.e. size, name, header information, date modified, etc.).
  - **Digital Fingerprints** - Recognition and identification of data/files are based on their digital fingerprints.
  - **Complex** - Recognition and identification of data/files are based on the content described by a Boolean expression of multiple rule types.
- **Action(s)** - Shows which user actions are allowed or disallowed on protocols and which user actions are logged to the Shadow Log.
- **Applies To** - Possible values:
  - **Permissions** - The rule applies to access control operations.
  - **Shadowing** - The rule applies to shadow copy operations.
  - **Detection** - The rule applies to content detection operations.
  - **Permissions+Shadowing** - The rule applies to both access control and shadow copy operations.
  - **Permissions+Detection** - The rule applies to both access control and detection operations.
  - **Shadowing+Detection** - The rule applies to both shadow copy and detection operations.
  - **Permissions+Shadowing+Detection** - The rule applies to all available operations: access control, shadow copy, and detection.

- **Protocol(s)** - The protocol(s) to which the rule applies.
  - **Send Alert** - Shows whether alerts are enabled or disabled for this rule.
  - **Log Event** - Shows whether the audit logging of events associated with this rule is enabled or disabled.
  - **Shadow Copy** - Shows whether the shadow copying is enabled or disabled for this rule.
  - **Profile** - Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to computers that are working offline.
- Different online vs. offline Content-Aware Rules can be defined for the same user(s) or groups of users. For information about how to define offline Content-Aware Rules for protocols, see [Managing Offline Content-Aware Rules for Protocols](#).

The shortcut menu on a rule in the details pane provides the following commands:

- **Manage** - Depending on the rule's profile (regular or offline), opens a dialog box to define the online (regular) or offline content-aware rules.
- **Edit** - Opens a dialog box to view or modify the rule.
- **Send Alert** - Enables or disables alerts for the given rule.
- **Log Event** - Enables or disables the audit logging of events associated with the given rule.
- **Shadow Copy** - Enables or disables the shadow copying of the content that causes the rule to trigger.
- **Delete** - Deletes the given rule.

For further details, see [Managing Content-Aware Rules](#).

## Access Control

By using Content-Aware Rules for protocols, one can do the following:

- Grant access to specified content when access is denied at the protocol-level.
- Deny access to specified content when access is granted at the protocol-level.

Content-Aware Rules apply to sessions allowed by the Protocols White List if the [Content Inspection](#) flag is selected. Otherwise, Content-Aware Rules have no effect on those sessions.

The following table provides summary information on access rights that can be specified for each protocol in Content-Aware Rules.

Protocol	Access rights	Description
Career Search	Generic: Search	Controls whether the user can submit vacancy search requests with specified content on job search sites.
	Generic: Outgoing Messages	Controls whether the user can send messages and submit résumé and other web-form data with specified content on job search sites.

	Generic: Outgoing Files	Controls whether the user can upload files with specified content to job search sites.
File Sharing, HTTP	Generic: POST Requests	Controls whether the user can submit Web form data with specified content to a Web server using HTTP.
	Generic: Outgoing Files	Controls whether the user can upload files with specified content to a Web server using HTTP.
	SSL: POST Requests	Controls whether the user can submit Web form data with specified content to a Web server using HTTPS.
	SSL: Outgoing Files	Controls whether the user can upload files with specified content to a Web server using HTTPS.
FTP	Generic: Outgoing Files	Controls whether the user can upload files with specified content to an FTP server.
	SSL: Outgoing Files	Controls whether the user can upload files with specified content to an FTP server using FTPS.
IBM Notes	Generic: Outgoing Messages	Controls whether the user can send email messages with specified content from the IBM Notes client to IBM Domino server.
	Generic: Outgoing Files	Controls whether the user can send email attachments with specified content from the IBM Notes client to IBM Domino server.
ICQ Messenger, IRC	Generic: Outgoing Messages	Controls whether the user can send instant messages with specified content.
	Generic: Outgoing Files	Controls whether the user can send files with specified content.
	SSL: Outgoing Messages	Controls whether the user can send instant messages with specified content using SSL.
	SSL: Outgoing Files	Controls whether the user can send files with specified content using SSL.
Mail.ru Agent,	Generic:	Controls whether the user can send instant messages with specified

Jabber, Skype, Zoom	Outgoing Messages	content.
	Generic: Outgoing Files	Controls whether the user can send files with specified content.
MAPI	Generic: Outgoing Messages	Controls whether the user can send email messages with specified content from the Outlook client to Microsoft Exchange Server.
	Generic: Outgoing Files	Controls whether the user can send email attachments with specified content from the Outlook client to Microsoft Exchange Server.
SMB	Generic: Outgoing Files	Controls whether the user can upload files with specified content to SMB servers and download such files from shared network folders of the computer running DeviceLock Service.
SMTP, Web Mail	Generic: Outgoing Messages	Controls whether the user can send email messages with specified content.
	Generic: Outgoing Files	Controls whether the user can send email attachments with specified content.
	SSL: Outgoing Messages	Controls whether the user can send email messages with specified content using SSL.
	SSL: Outgoing Files	Controls whether the user can send email attachments with specified content using SSL.
Social Networks	Generic: Outgoing Messages	Controls whether the user can send messages, comments, and posts with specified content.
	Generic: Outgoing Files	Controls whether the user can send media and other files with specified content to a social networking site.
Viber	Generic: Outgoing Files	Controls whether the user can send files with specified content.
Web Search	Generic: Search	Controls whether the user can submit search requests with specified content on web search sites.

---

## Note

- If the “No Access” permission is set for a protocol and there is a Content-Aware Rule that allows access to specified content for the same protocol, the Send/Receive Data access right is automatically granted to users for this protocol. For more information about this access right, see [Managing Permissions for Protocols](#).
  - If the “No Access” permission is set for the **Viber** protocol, Content-Aware Rules that allow access to specified content for that protocol have no effect. In this case, the Viber user can neither send nor receive messages and files.
  - The **POST Requests** access right for the **File sharing** protocol, when applied to the iCloud service, controls whether a user can upload non-file data (Mail, Notes, Calendar, Contacts, Reminders) to iCloud. The same access right enables the audit logging and shadow copying of the non-file data uploaded to iCloud. Audit records of upload attempts and shadow copies of that data are stored as **Outgoing Messages**.
  - The access rights for the **MAPI** protocol also apply to the drafts of the messages not sent from Outlook to Exchange Server. For example, DeviceLock will not allow Outlook to auto-save message drafts with specified content if the Outlook user does not have the right to send messages with that content.
- 

When using Content-Aware Rules, consider the following:

- Content-Aware Rules with **Deny** settings take priority over rules with **Allow** settings if they apply to the same users or groups.  
Exception: Content-Aware Rules with Allow settings based on a Document Properties group with the **Text extraction not supported** option selected take priority over rules with **Deny** settings and allow transfer of any matching content, including split (or multi-volume) archives.  
Exception: An **Allow** Content-Aware Rule based on a Document Properties group with the **Password protected** option selected takes priority over **Deny** rules (if any) and allows transfer of any matching content. A Complex **Allow** Content-Aware Rule Boolean will take priority only if there is a Document Properties group with the **Password protected** option selected among a set of logically connected content groups that the file matched.  
Exception: An **Allow** Content-Aware Rule based on a Digital Fingerprints group with the **Exact file match** option selected takes priority over **Deny** rules (if any) and allows transfer of any matching content. A Complex **Allow** Content-Aware Rule Boolean will take priority only if there is a Digital Fingerprints group with the **Exact file match** option selected among a set of logically connected content groups that the file matched.
- Content-Aware Rules with **Allow** settings allow transfer of the whole data object (message or file, including archives and other containers) when the content matches these rules and when the content does not match a Content-Aware Rule with **Deny** settings.
- Checking the content of files can be a time-consuming operation. The DeviceLock administrator can define a content verification message to be displayed to users when content inspection is in progress. For detailed information on this message, see the [Content verification message](#) parameter description in [Service Options](#).

- When Content-Aware Rules block transmitting certain content, the user is notified by a message, provided that the respective message is enabled in [Service Options](#). For detailed information on this message, see the [Content-Aware blocked write message](#) parameter description.

## Content-Aware Shadowing

Before Content-Aware Rules can be used for shadow copy operations, one must turn on shadowing in **Auditing, Shadowing and Alerts** at the protocol-level. Content-Aware Rules that apply to shadow copy operations filter the shadow copies of data and files transmitted by the user.

The following table provides summary information on shadowing rights that can be specified for each protocol in Content-Aware Rules.

Protocol	Shadowing rights	Description
Career Search	Generic: Search	Controls whether to create shadow copy of vacancy search requests with specified content submitted on job search sites.
	Generic: Outgoing Messages	Controls whether to create shadow copy of messages, résumé and other web-form data with specified content submitted on job search sites.
	Generic: Outgoing Files	Controls whether to create shadow copy of files with specified content uploaded to job search sites.
File Sharing, HTTP	Generic: Incoming Files	Controls whether to create shadow copy of files with specified content downloaded from a Web server.
	Generic: Outgoing Files	Controls whether to create shadow copy of files with specified content uploaded to a Web server.
	Generic: POST Requests	Controls whether to create shadow copy of Web form data with specified content submitted to a Web server.
	SSL: Incoming Files	Controls whether to create shadow copy of files with specified content downloaded from a Web server using HTTPS.
	SSL: Outgoing Files	Controls whether to create shadow copy of files with specified content uploaded to a Web server using HTTPS.
	SSL: POST Requests	Controls whether to create shadow copy of Web form data with specified content submitted to a Web server using HTTPS.

### Note

The POST Requests right for the File Sharing protocol, when applied to the iCloud service, enables the shadow copying of non-file data (Mail, Notes, Calendar, Contacts, Reminders).

FTP	Generic: Incoming Files	Controls whether to create shadow copy of files with specified content downloaded from an FTP server.
	Generic: Outgoing	Controls whether to create shadow copy of files with specified



	Files	content uploaded to an FTP server.
	SSL: Incoming Files	Controls whether to create shadow copy of files with specified content downloaded from an FTP server using FTPS.
	SSL: Outgoing Files	Controls whether to create shadow copy of files with specified content uploaded to an FTP server using FTPS.
IBM Notes	Generic: Incoming Messages	Controls whether to create shadow copy of email messages with specified content received by the user to the IBM Notes client from IBM Domino server.
	Generic: Incoming Files	Controls whether to create shadow copy of email attachments with specified content received by the user to the IBM Notes client from IBM Domino server.
	Generic: Outgoing Messages	Controls whether to create shadow copy of email messages with specified content sent by the user from the IBM Notes client to IBM Domino server.
	Generic: Outgoing Files	Controls whether to create shadow copy of email attachments with specified content sent by the user from the IBM Notes client to IBM Domino server.
ICQ Messenger, IRC	Generic: Incoming Messages	Controls whether to create shadow copy of instant messages with specified content received by the user.
	Generic: Incoming Files	Controls whether to create shadow copy of files with specified content received by the user.
	Generic: Outgoing Messages	Controls whether to create shadow copy of instant messages with specified content sent by the user.
	Generic: Outgoing Files	Controls whether to create shadow copy of files with specified content sent by the user.
	SSL: Incoming Messages	Controls whether to create shadow copy of instant messages with specified content received by the user using SSL.
	SSL: Incoming Files	Controls whether to create shadow copy of files with specified content received by the user using SSL.
	SSL: Outgoing Messages	Controls whether to create shadow copy of instant messages with specified content sent by the user using SSL.
	SSL: Outgoing Files	Controls whether to create shadow copy of files with specified content sent by the user using SSL.
Jabber, Mail.ru Agent, Skype, Telegram, Viber, WhatsApp, Zoom	Generic: Incoming Messages	Controls whether to create shadow copy of instant messages with specified content received by the user.
	Generic: Incoming Files	Controls whether to create shadow copy of files with specified content received by the user.

MAPI	Generic: Outgoing Messages	Controls whether to create shadow copy of instant messages with specified content sent by the user.
	Generic: Outgoing Files	Controls whether to create shadow copy of files with specified content sent by the user.
	Generic: Incoming Messages	Controls whether to create shadow copy of email messages with specified content received by the user to the Outlook client from Microsoft Exchange Server.
	Generic: Incoming Files	Controls whether to create shadow copy of email attachments with specified content received by the user to the Outlook client from Microsoft Exchange Server.
	Generic: Outgoing Messages	Controls whether to create shadow copy of email messages with specified content sent by the user from the Outlook client to Microsoft Exchange Server.
SMB	Generic: Outgoing Files	Controls whether to create shadow copy of email attachments with specified content sent by the user from the Outlook client to Microsoft Exchange Server.
	Generic: Incoming Files	Controls whether to create shadow copy of files with specified content the user downloads from SMB servers or uploads to shared network folders on the computer running DeviceLock Service.
SMTP, Web Mail	Generic: Outgoing Files	Controls whether to create shadow copy of files with specified content the user uploads to SMB servers or downloads from shared network folders on the computer running DeviceLock Service.
	Generic: Outgoing Messages	Controls whether to create shadow copy of email messages with specified content sent by the user.
	Generic: Outgoing Files	Controls whether to create shadow copy of email attachments with specified content sent by the user.
	SSL: Outgoing Messages	Controls whether to create shadow copy of email messages with specified content sent by the user using SSL.
Social Networks	SSL: Outgoing Files	Controls whether to create shadow copy of email attachments with specified content sent by the user using SSL.
	Generic: Outgoing Messages	Controls whether to create shadow copy of messages, comments, and posts with specified content sent by the user.
Web Search	Generic: Outgoing Files	Controls whether to create shadow copy of media and other files with specified content uploaded to a social networking site.
	Generic: Search	Controls whether to create shadow copy of web search requests with specified content.

## Content-Aware Detection

The following table provides summary information on detection rights that can be specified in Content-Aware Rules.

Protocol	Access rights	Description
Career Search	Generic: Search	Controls whether to detect user attempts to submit vacancy search requests with specified content on job search sites.
	Generic: Outgoing Messages	Controls whether to detect user attempts to send messages or submit résumé and other web-form data with specified content on job search sites.
	Generic: Outgoing Files	Controls whether to detect user attempts to upload files with specified content to job search sites.
File Sharing, HTTP	Generic: Incoming Files	Controls whether to detect user attempts to download files with specified content from a Web server using HTTP.
	Generic: POST Requests	Controls whether to detect user attempts to submit Web form data with specified content to a Web server using HTTP.
	Generic: Outgoing Files	Controls whether to detect user attempts to upload files with specified content to a Web server using HTTP.
	SSL: Incoming Files	Controls whether to detect user attempts to download files with specified content from a Web server using HTTPS.
	SSL: POST Requests	Controls whether to detect user attempts to submit Web form data with specified content to a Web server using HTTPS.
	SSL: Outgoing Files	Controls whether to detect user attempts to upload files with specified content to a Web server using HTTPS.
FTP	Generic: Incoming Files	Controls whether to detect user attempts to download files with

		specified content from an FTP server.
	Generic: Outgoing Files	Controls whether to detect user attempts to upload files with specified content to an FTP server.
	SSL: Incoming Files	Controls whether to detect user attempts to download files with specified content from an FTP server using FTPS.
	SSL: Outgoing Files	Controls whether to detect user attempts to upload files with specified content to an FTP server using FTPS.
IBM Notes	Generic: Incoming Messages	Controls whether to detect user attempts to receive email messages with specified content from IBM Domino server to the IBM Notes client.
	Generic: Incoming Files	Controls whether to detect user attempts to receive email attachments with specified content from IBM Domino server to the IBM Notes client.
	Generic: Outgoing Messages	Controls whether to detect user attempts to send email messages with specified content from the IBM Notes client to IBM Domino server.
	Generic: Outgoing Files	Controls whether to detect user attempts to send email attachments with specified content from the IBM Notes client to IBM Domino server.
ICQ Messenger, IRC	Generic: Incoming Messages	Controls whether to detect user attempts to receive instant messages with specified content.
	Generic: Incoming Files	Controls whether to detect user attempts to receive files with specified content.
	Generic: Outgoing Messages	Controls whether to detect user attempts to send instant messages with specified content.
	Generic: Outgoing Files	Controls whether to detect user attempts to send files with specified content.
	SSL: Incoming Messages	Controls whether to detect user

		attempts to receive instant messages with specified content using SSL.
	SSL: Incoming Files	Controls whether to detect user attempts to receive files with specified content using SSL.
	SSL: Outgoing Messages	Controls whether to detect user attempts to send instant messages with specified content using SSL.
	SSL: Outgoing Files	Controls whether to detect user attempts to send files with specified content using SSL.
Jabber, Mail.ru Agent, Skype, Telegram, Viber, WhatsApp, Zoom	Generic: Incoming Messages	Controls whether to detect user attempts to receive instant messages with specified content.
	Generic: Incoming Files	Controls whether to detect user attempts to receive files with specified content.
	Generic: Outgoing Messages	Controls whether to detect user attempts to send instant messages with specified content.
	Generic: Outgoing Files	Controls whether to detect user attempts to send files with specified content.
MAPI	Generic: Incoming Messages	Controls whether to detect user attempts to receive email messages with specified content from Microsoft Exchange Server to Outlook.
	Generic: Incoming Files	Controls whether to detect user attempts to receive email attachments with specified content from Microsoft Exchange Server to Outlook.
	Generic: Outgoing Messages	Controls whether to detect user attempts to send email messages with specified content from Outlook to Microsoft Exchange Server.
	Generic: Outgoing Files	Controls whether to detect user attempts to send email attachments with specified content from Outlook to Microsoft Exchange Server.

---

**Note**

The detection-related rights for the MAPI protocol also apply to the drafts of the messages not sent from Outlook to Exchange Server. Thus, if the Outlook user has the right to send messages with specified content, DeviceLock would detect the saved draft of such a message when the user closes Outlook without sending the message. If the user does not have that right, the message with specified content would be detected when saving the message draft in Outlook.

---

SMB	Generic: Incoming Files	Controls whether to detect user attempts to download files with specified content from SMB servers or upload such files to shared network folders on the computer running DeviceLock Service.
	Generic: Outgoing Files	Controls whether to detect user attempts to upload files with specified content to SMB servers or download such files from shared network folders on the computer running DeviceLock Service.
SMTP, Web Mail	Generic: Outgoing Messages	Controls whether to detect user attempts to send email messages with specified content.
	Generic: Outgoing Files	Controls whether to detect user attempts to send email attachments with specified content.
	SSL: Outgoing Messages	Controls whether to detect user attempts to send email messages with specified content using SSL.
	SSL: Outgoing Files	Controls whether to detect user attempts to send email attachments with specified content using SSL.
Social Networks	Generic: Outgoing Messages	Controls whether to detect user attempts to send messages, comments, and posts with specified content.
	Generic: Outgoing Files	Controls whether to detect user attempts to send media files or other files with specified content to a social networking site.
Web Search	Generic: Search	Controls whether to detect user attempts to submit search requests with specified content on web search

sites.

## Configuring Content Groups

Content-Aware Rules are created based on content groups that provide the ability to centrally define types of content for which access control is desired. Content groups specify content filtering criteria for identifying data to which rules should be applied.

All content groups are stored in the Content Database. The same Content Database is used for both devices and protocols. The Content Database is a part of the DeviceLock Service policy and is also saved in a file with DeviceLock Service settings that can be created using DeviceLock Management Console, DeviceLock Service Settings Editor, and the DeviceLock Group Policy Manager.

The following topics describe the content group types that are available, and provide instructions on how to create custom content groups of each type:

- [File Type Detection Content Groups](#) - Identify files by using file type-specific signatures.
- [Keywords Content Groups](#) - Look for specific keywords or phrases in data/files.
- [Pattern Content Groups](#) - Look for specific text fragments by using Perl regular expressions.
- [Document Properties Content Groups](#) - Look for document properties, such as size, name, title, subject, etc.
- [Digital Fingerprints Content Groups](#) - Check digital fingerprints of data/files.
- [Complex Content Groups](#) - Compose a logical expression of multiple group types.

Configuring content groups also involves the following tasks:

- [Viewing Built-in Content Groups](#)
- [Duplicating Built-in Content Groups](#)
- [Editing or Deleting Custom Content Groups](#)
- [Testing Content Groups](#)

## File Type Detection Content Groups

File Type Detection groups are used to control access to files based on their true file types as detected and differentiated from other file types based on binary analysis and not just the file name or type attributes. For selection purposes, these File Type Detection group memberships contain common definitions of the file types that make up these groups. A file type definition consists of two display properties: a file name extension (for example, DOC) and a description (for example, Microsoft Word document). When DeviceLock applies a rule based on a File Type Detection group, the rule is applied to all file types included in that group.

DeviceLock includes more than 30 predefined (built-in) File Type Detection groups that can be used to set up the desired configuration of permissions and/or shadow copy operations. Administrators can use built-in groups as they are, create their editable copies (duplicates), or create their own custom groups to suit a particular organization's needs.

Built-in groups make it easy to configure rules without necessarily having to define custom content groups.

---

**Note**

It is possible to view the settings in each built-in group; however, built-in groups cannot be modified or deleted. For more information and instructions, see [Viewing Built-in Content Groups](#).

---

The following table lists all built-in content groups of this type:

Built-in File Type Detection groups	
Android	MS OneNote
Archives	MS Outlook, Outlook Express & Email archives
Audio, Video & Flash	MS PowerPoint
BlackBerry	MS Project
Common Object File Format (COFF)	MS Publisher
Database	MS Visio
Executable	MS Windows Installer
Fax Documents	MS Windows Memory Dump
FileMaker Pro	MS Word
Fonts	MS Works
Help Files	OpenOffice, StarOffice, OpenDocument, etc.
Images, CAD & Drawing	PDF, PostScript, & XPS Documents
iOS	QuickBooks, Quicken, TurboTax & etc.
Lotus SmartSuite	Rich Text Format
MS Access	Security Certificates
MS Excel	Text, HTML & XML
MS InfoPath	Virtual Machines
MS Money	WordPerfect Office



---

**Note**


- Content-Aware Rules support Word To Go, Sheet To Go, and Slideshow To Go formats for Palm devices. Word To Go format is included in the MS Word and Rich Text Format built-in content groups, Sheet To Go format is included in the MS Excel built-in content group, while Slideshow To Go format is included in the MS PowerPoint built-in content group.
  - Microsoft Word or Rich Text Format (RTF) files, Excel files, and PowerPoint files can be transferred to a Palm device using the Documents To Go application that converts those files to special formats: Word and RTF files are converted to Word To Go format, Excel files are converted to Sheet To Go format, PowerPoint files are converted to Slideshow To Go format. The converted files are automatically downloaded to the Palm when users synchronize.
- 

## Creating Custom File Type Detection Groups

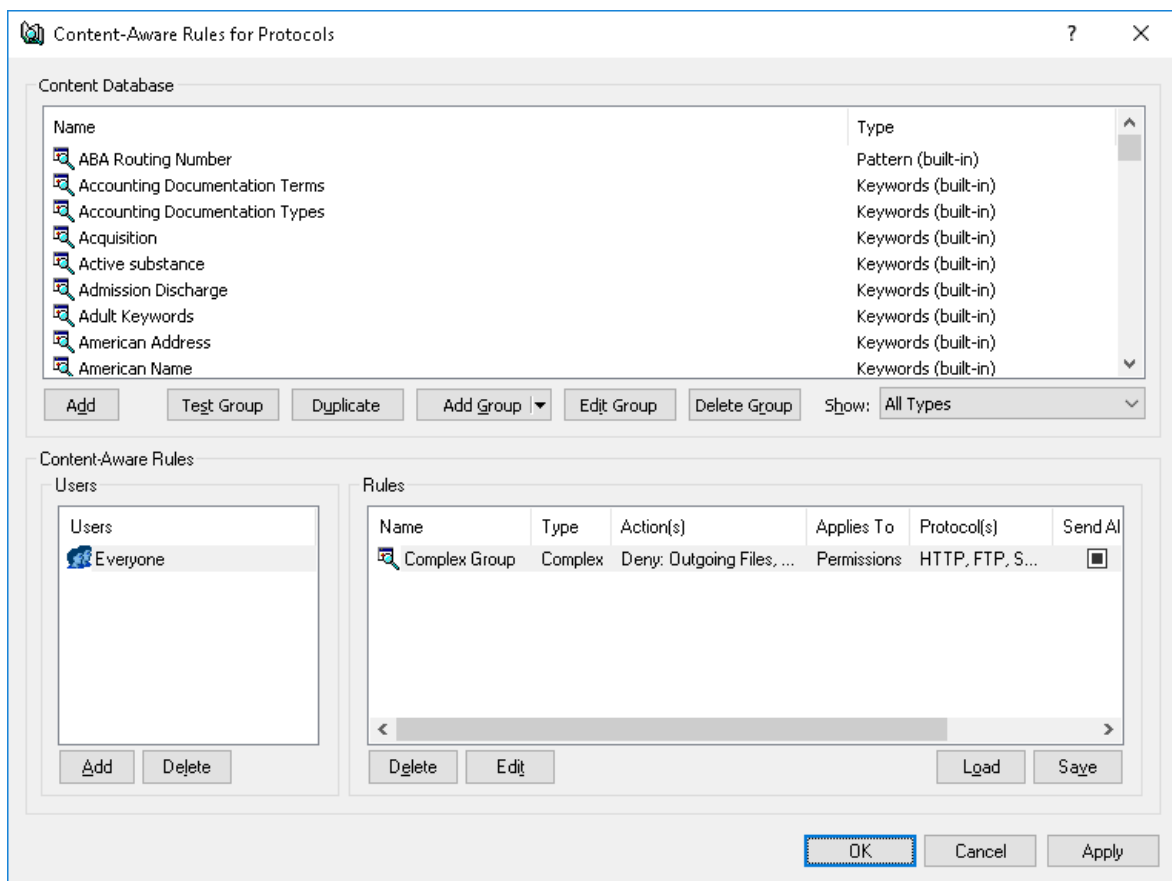
One can define Content-Aware Rules based on custom content groups if the predefined content groups included with DeviceLock do not meet desired requirements. Custom File Type Detection content groups enable administrators to specify any file types that are desired to be in the same group to better meet individual business needs.

For example, suppose it is desired to grant certain users access to Word, Excel, PDF documents and graphic files. To do this, first create a new File Type Detection content group that represents these document content types. Then, define a rule based on this custom content group.

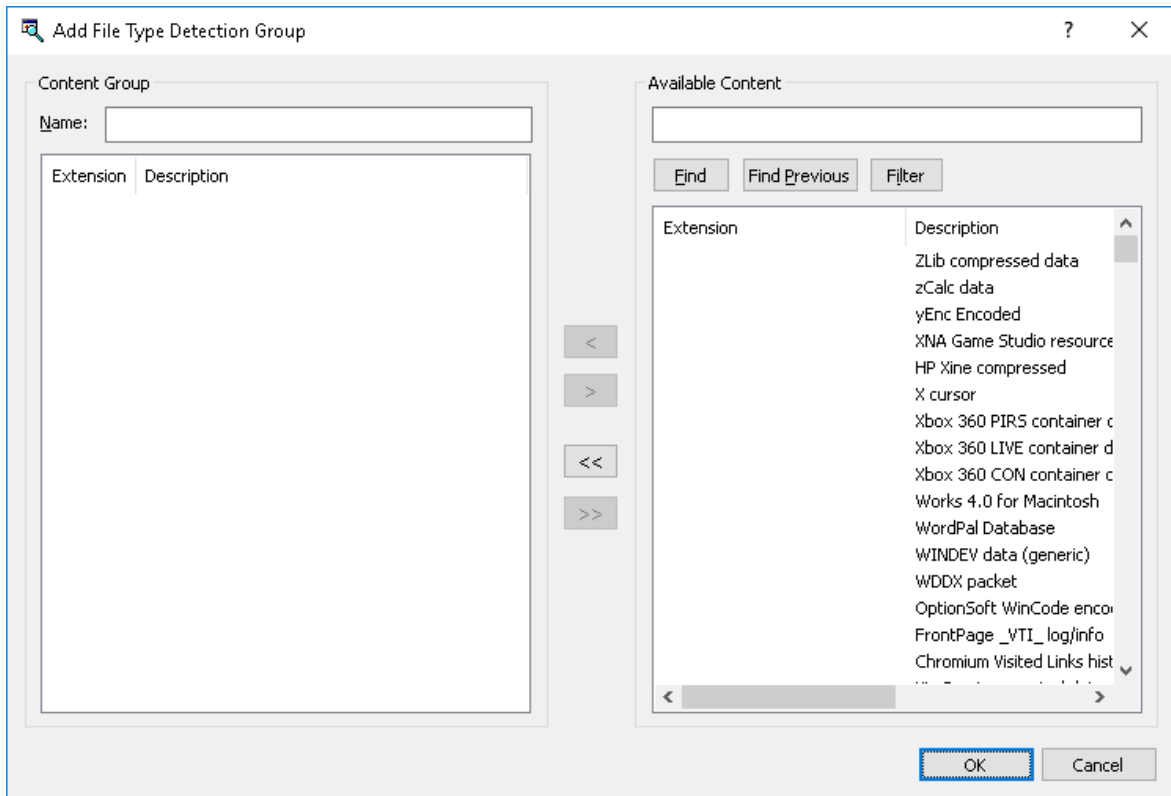
### ***To create a custom File Type Detection group***


1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand either the **Devices** or **Protocols** node.
3. Under the **Devices** or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.
  - OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.




*This will display a dialog box similar to the following.*



- In the upper pane of the dialog box that appears, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **File Type Detection**.  
*This will display the Add File Type Detection Group dialog box.*



5. In the left pane of the **Add File Type Detection Group** dialog box, under **Content group**, type the name of the new content group in the **Name** box.
6. In the right pane of the **Add File Type Detection Group** dialog box, under **Available Content**, select any file type desired to add to the new content group, and then click the left single-arrow button .

*You can select multiple file types by holding down the SHIFT key or the CTRL key while clicking them. To remove single file types from the content group, use the right single-arrow button . To add or remove all available file types to or from the content group at the same time, use the left double-arrow button  or right double-arrow button .*

### Note

It is possible to search the available content database for specific file types by extension or description. Wildcards such as asterisks (\*) and question marks (?) can be used to search for a specific group of file types. To find a specific file type or specific group of file types, under **Available Content**, type an extension or description with or without wildcards in the search string, and then click **Find**. To filter file types, click **Filter**. To remove the filter, apply it to an empty string.

An asterisk (\*) replaces an unlimited number of characters. The question mark (?) replaces a single positional character. Wildcards can be used in any position and in any quantity.

7. Click **OK** to close the **Add File Type Detection Group** dialog box.  
*The new content group created is added to the existing list of content groups under Content Database in the upper pane of the dialog box for managing content-aware rules.*

## Keywords Content Groups

Keywords groups are used to control access to data/files based on specified keywords or phrases.

DeviceLock includes more than 160 predefined (built-in) Keywords groups that can be used to set up the desired configuration of permissions and/or shadow copy operations. It is possible to use the built-in content groups as they are, create their editable copies (duplicates), or create custom content groups to suit a particular organization's needs.

Built-in content groups make it easy to configure rules without necessarily having to define custom content groups.

---

### Note

It is possible to view the settings in each built-in group; however, built-in groups cannot be modified or deleted. For more information and instructions, see [Viewing Built-in Content Groups](#).

---

The following table lists all built-in content groups of this type:

Built-in Keywords groups	
Accounting Documentation Terms	Project Names
Accounting Documentation Types	Project Release Dates
Acquisition	Property
Active substance	Racism Keywords
Admission Discharge	Resume
Adult Keywords	Russian: Account Statement
American Address	Russian: Accounting Documentation
American Name	Russian: Accounting Documentation Terms
Bank ABA	Russian: Accounting Documentation Types
Bank ACNT	Russian: Bank Account
Bank STMT	Russian: Bank Operations
Board Meeting	Russian: Banking Operations Participants
Breach of Obligation	Russian: Breach of Commitment
Breach of Standards	Russian: Breach of Law
Breach of the Law	Russian: Business Documentation
Business Documentation	Russian: Business Documentation Terms
Business Documentation Terms	Russian: Business Documentation Types

Business Documentation Types	Russian: Business Partners
Business Rivals	Russian: Business Trips & Meetings
Business Trips & Meetings	Russian: Company Development Plan
C# Source Code	Russian: Compensation and Benefits
C/C++ Source Code	Russian: Confidential Information
Cellular Operator Call Log	Russian: Corporate Capital
COBOL Source Code	Russian: Corporate Legal Documentation
Common Disease	Russian: Corporate Property
Common Medical Terms	Russian: Expenses
Company Development	Russian: Failures
Compensation and Benefits	Russian: Financial Information
Compliance Report	Russian: Financial Report
Confidential	Russian: Financial Terms
Confidential Partners Information	Russian: Firing
Credit Report	Russian: HR Department Documentation
Credits	Russian: Innovations
Discontent	Russian: Insurance
Discrediting Information	Russian: Internal Payments
Driver's License	Russian: International Economic Activity
Employer Identification Number	Russian: Investors and Investments
Ethnicity	Russian: IT Department Documentation
Executive Job Searches	Russian: Labor Law
Failures	Russian: Loans and Credits
Financial Report	Russian: Manufacturing
Financial Statements	Russian: Market Development Plan
Firing	Russian: Medical Terms
FITS Date & Time	Russian: Medicinal Active Substances
FITS File Checksum	Russian: Medicinal Drugs
FITS File Descriptors	Russian: Noncompliant
FITS Hierarchical file grouping	Russian: Obscene Language


FITS Instrumentorum	Russian: Passwords and Access Codes
FITS Non-standard	Russian: Patents and Trademarks
FITS Observations	Russian: Physical Security
FITS Standard	Russian: Prices
Gambling	Russian: Project Documentation
Grades	Russian: Project Names
HCFA (CMS) 1500 Form	Russian: Project Versions
HIPAA - Diseases	Russian: Projects Release Date
HIPAA HCPCS	Russian: Racism Keywords
HIPAA ICD 10 - Diseases and Injuries	Russian: Technology
HIPAA ICD 10 - Drugs and Chemicals	Russian: Tender Documentation
HIPAA ICD9	Russian: User Names
HIPAA NDC Classes	Russian: Violence
HIPAA NDC Dosages	Russian: Working Conditions
HIPAA NDC Listing	Sales Forecast
HIPAA NDC Routes	Sarbanes-Oxley Sensitive
Illegal Drugs	Security
Innovations	Security Agencies
Internet Slang Abbreviations	Sensitive Disease
Investments	Sexual Language
Java Source Code	Social Security
Japan: Surname in Hiragana	SPAM
Japan: Surname in Kanji	Prices
Japan: Surname in Katakana	Pro Earnings
Japan: Surname in One-Byte-Katakana	Sports
Market Development	Staff Training
Medical Diagnosis	Substance Abuse
Medical Record Numbers	Suspicious Activity Report
MEMO	Technology
Network Security	UBO4 Form

Partner Names	US Birth Date
Password	US Birth Place
Payments	US Expiry Date
PCI GLBA	User Name
Perl Source Code	VB Source Code
Price List	Violence
Production Charges	Weapon Keywords
Profanity	Wire Transfer
Profiles	Working Conditions
Profit Loss	

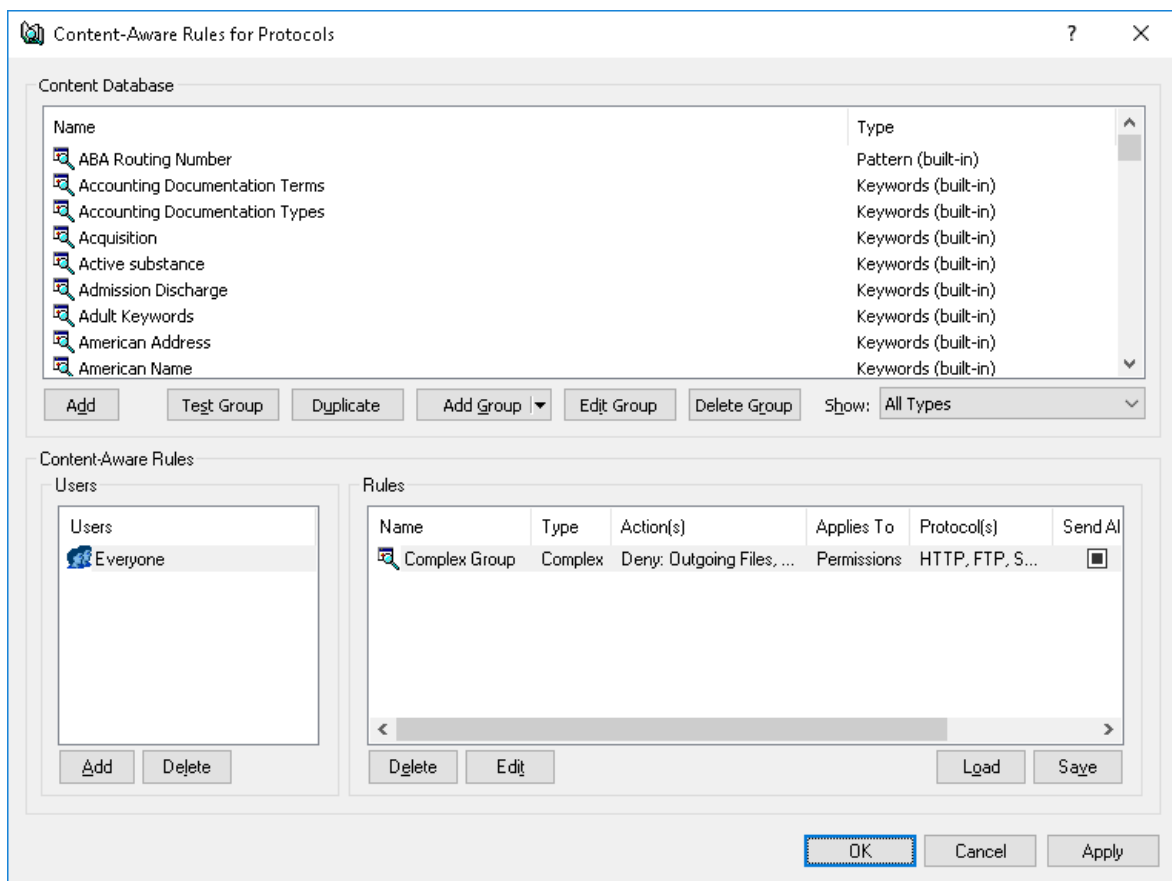
## Creating Custom Keywords Groups

One can define Content-Aware Rules based on custom content groups if the predefined content groups included with DeviceLock do not meet desired requirements. Custom Keywords content groups enable administrators to specify any keywords that are desired to be in the same group to better meet individual business needs.

### ***To create a custom Keywords group***

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand either the **Devices** or **Protocols** node.
3. Under the **Devices** or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.
  - OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.

*This will display a dialog box similar to the following.*



- In the upper pane of the dialog box that appears, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Keywords**.  
*This will display the Add Keywords Group dialog box.*



**Add Keywords Group**

Name:

Description:

Condition: Only when combined score exceeds (or equal to) threshold Threshold:

Keywords	Case Sensitive	Whole Word	Word Forms	Weight
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Normal

☐ OCR

NOTE: Selection of multiple languages marked with an asterisk (\*) or singular asterisk-marked selections combined with any selection of unmarked languages may cause a performance degradation of the OCR processing engine.

☐ Count identical matches as one match

5. In the **Add Keywords Group** dialog box, do the following:
  - **Name** - Specify the name of the group.
  - **Description** - Specify a description for the group.
  - **Condition** - Specify conditions for firing rules associated with this content group. To do so, in the **Condition** list, click any of the following options:
    - **Match any keyword(s)** - A rule associated with this content group fires every time ANY of the specified keywords is found within text data.
    - **Match all keyword(s)** - A rule associated with this content group fires every time ALL of the specified keywords are found within text data.
    - **Only when combined score exceeds (or equal to) threshold** - A rule associated with this content group fires every time the total number (sum) of occurrences (i.e. "hits") of all found keywords within text data equals or exceeds the threshold number of occurrences of the keywords.
  - **Threshold** - Specify the threshold number of occurrences (i.e. "hits") of the keywords. This number can range from 0 to 65535. This property requires a value if the **Only when combined score exceeds (or equal to) threshold** option is selected.
  - **Keywords** - Specify words and phrases that must occur within text data. Double-click under **Keywords** to enter a keyword or phrase.
  - **Case Sensitive** - Determine the case sensitivity of the keywords. Select the **Case Sensitive** check box to specify a case-sensitive comparison of the keywords (for example, the words test and Test will be treated as different keywords).

Clear the **Case Sensitive** check box to specify a case-insensitive comparison of the keywords (for example, the words test and Test will be treated as the same keyword).

- **Whole Word** - Set keyword matching options. Select the **Whole Word** check box to specify the exact keyword match option.

Clear the **Whole Word** check box to specify the broad match option, which then finds all grammatical variations of the desired keyword.

- **Word Forms** - Provides for the morphological search that takes into account various grammar forms of keywords. Select this check box to enable the morphological search in Catalan, English, French, German, Italian, Polish, Portuguese, Russian, and Spanish languages. When this check box is selected, it also enables the search for Russian words transliterated using Latin characters as well as the search that accounts for possible replacement of certain characters with other ones similar in appearance or meaning, including:

- Latin characters in the Russian text (such as Latin b in place of Russian б)
- Latin characters in place of certain numerals (such as Latin s in place of digit 5)
- Russian characters in the English text (such as Russian n in place of Latin n)
- Russian characters in place of certain numerals (such as Russian 3 in place of digit 3)
- Certain symbols in place of Russian characters (such as \* (asterisk) in place of Russian ж)
- Numerals in place of certain Latin or Russian characters (such as digit 1 in place of Latin I or digit 4 in place of Russian ч)
- Arabic-Indic (Eastern Arabic) numerals in place of normal Arabic numerals (such as symbol ٣ in place of digit 3 or symbol ٨ in place of digit 8)

*The morphological search can be time-consuming and resource-intensive.*

Clear the **Word Forms** check box to search for keywords without accounting for the morphology, transliteration, and substitution of characters.

- **Weight** - Specify the degree of importance for each keyword or phrase. Weight is used to count the number of occurrences of the specified keywords within text data. This property requires a value if the **Only when combined score exceeds (or equal to) threshold** option is selected.

Possible values: **Heavy**, **Above Normal**, **Normal** (default value), **Below Normal**, **Light**. These weight values are interpreted as follows:

- **Heavy** - Each keyword occurrence is counted as three occurrences. This value is the highest.
  - **Above Normal** - Each keyword occurrence is counted as two occurrences.
  - **Normal** - Each keyword occurrence is counted as one occurrence.
  - **Below Normal** - Two keyword occurrences are counted as one occurrence.
  - **Light** - Three keyword occurrences are counted as one occurrence. This value is the lowest.
- **Add** - Specify keywords and phrases. Click **Add** to enter a keyword or phrase.
  - **Delete** - To delete a keyword, select the keyword, and then click **Delete**.  
*You can select multiple keywords by holding down the SHIFT key or the CTRL key while clicking them.*
  - **Load** - Import keywords from a text file. Each keyword in this file must be on a separate line, with a line break after the last character of the keyword.

- **OCR** - Extract text from images for further checking against the list of keywords defined in this content group. To do so, select the **OCR** check box and up to 8 languages.

---

**Note**

Selection of multiple Asian languages (marked with an asterisk (\*) in the GUI) or singular Asian language selections combined with any selection of non-Asian languages may cause a performance degradation of the OCR processing engine.

---

For optimal performance and recognition quality, we recommend selecting only those languages that are really needed.

- **Count identical matches as one match** - Combine duplicate matches of a keyword into a single match. To do so, select the **Count identical matches as one match** check box. This parameter is active when the **Only when combined score exceeds (or equal to) threshold** option is selected.

6. Click **OK** to close the **Add Keywords Group** dialog box.

*The new content group created is added to the existing list of content groups under Content Database in the upper pane of the dialog box for managing content-aware rules.*

## Pattern Content Groups

Pattern groups are intended to control access to text data using patterns of alphanumeric text described by Perl regular expressions. Patterns provide a flexible and powerful way to automatically detect potentially sensitive content (for example, credit card numbers, Social Security numbers, email addresses, and phone numbers) within text data. For more information on creating and using Perl regular expressions, refer to the tutorials at [perldoc.perl.org/perlrequick.html](http://perldoc.perl.org/perlrequick.html) and [perldoc.perl.org/perlretut.html](http://perldoc.perl.org/perlretut.html).

DeviceLock includes more than 75 predefined (built-in) Pattern groups that can be used to set up the desired configuration of permissions and/or shadow copy operations. It is possible to use the built-in content groups as they are, create their editable copies (duplicates), or create custom content groups to suit a particular organization's needs.

Built-in content groups make it easy to configure rules without necessarily having to define custom content groups.

---

**Note**

It is possible to view the settings in each built-in group; however, built-in groups cannot be modified or deleted. For more information and instructions, see [Viewing Built-in Content Groups](#).

---

The following table lists all built-in content groups of this type:

Built-in Pattern groups	
ABA Routing Number	Russian: Employment Record Book Number
American Name (Ex)	Russian: Health Insurance Number

Austria SSN	Russian: International Passport
BIC (ISO 9362)	Russian: KPP
Bulgarian: EGN	Russian: Main State Registration Number
Californian ID Number	Russian: Motorcycle Numbers
Canadian Postal Code	Russian: OGRNIP
Canadian Social Insurance Number	Russian: OKATO
China National ID	Russian: OKFS
Credit Card Dump	Russian: OKOGU
Credit Card Number	Russian: OKOPF
Danish Personal ID	Russian: Passport
Dollar Amount	Russian: Passport Issuer Department Code
Dominican Republic ID Number	Russian: Pension Insurance Number
Email Address	Russian: Post Code
European VAT Number	Russian: Social Card
Finnish ID	Russian: Taxpayer Identification Number
France INSEE Code	Russian: Telephone Number
French NINO	Russian: Trailer Numbers
German eTIN	Russian: Vehicle Registration Document
German Telephone Number	Scotland CHI
GPS Data (RMC String)	South African ID Number
Health Insurance Claim	South Korean Resident Registration Number
IBAN	Spanish DNI
International Telephone Number	Spanish Full Name
IP Address	Spanish NIF
Irish PPSN	Spanish SSN
Irish VAT	SQL Queries
ISO Date	Sweden Personal ID
Japan: Address	Sweden Phone Number
Japan: Date	Sweden Post Code
Japan: Phone Number	Taiwan: ID Number


Japan: Social Security and Tax Number System	Taiwan: Jih Sun Bank Account Number
MAC Address	TCP/UDP Port Number
Mexican Tax ID Number	Time (12/24h)
Microsoft Windows Product Key	Turkish ID Number
National Provider Identifier	UK Date
Norwegian Birth Number	UK National Insurance Number
Poland National Identity Card Number	UK NHS Number
Polish ID Number	UK Phone Number
RAMQ	UK Post Code
Russian: Address	UK RD&E Hospital Number
Russian: Auto Insurance Number	UK Tax Code
Russian: Bank Account Number	Uniform Resource Locator (URL)
Russian: BIC	US Date
Russian: Car Numbers	US Phone Number
Russian: Classification of Economic Activities	US Social Security Number
Russian: Classification of Enterprises and Organizations	US Zip Code
Russian: Correspondent Account	US/UK Home Address
Russian: Diplomatic Passport	USSR Passport
Russian: Driver's License Number	VIN

## Creating Custom Pattern Groups

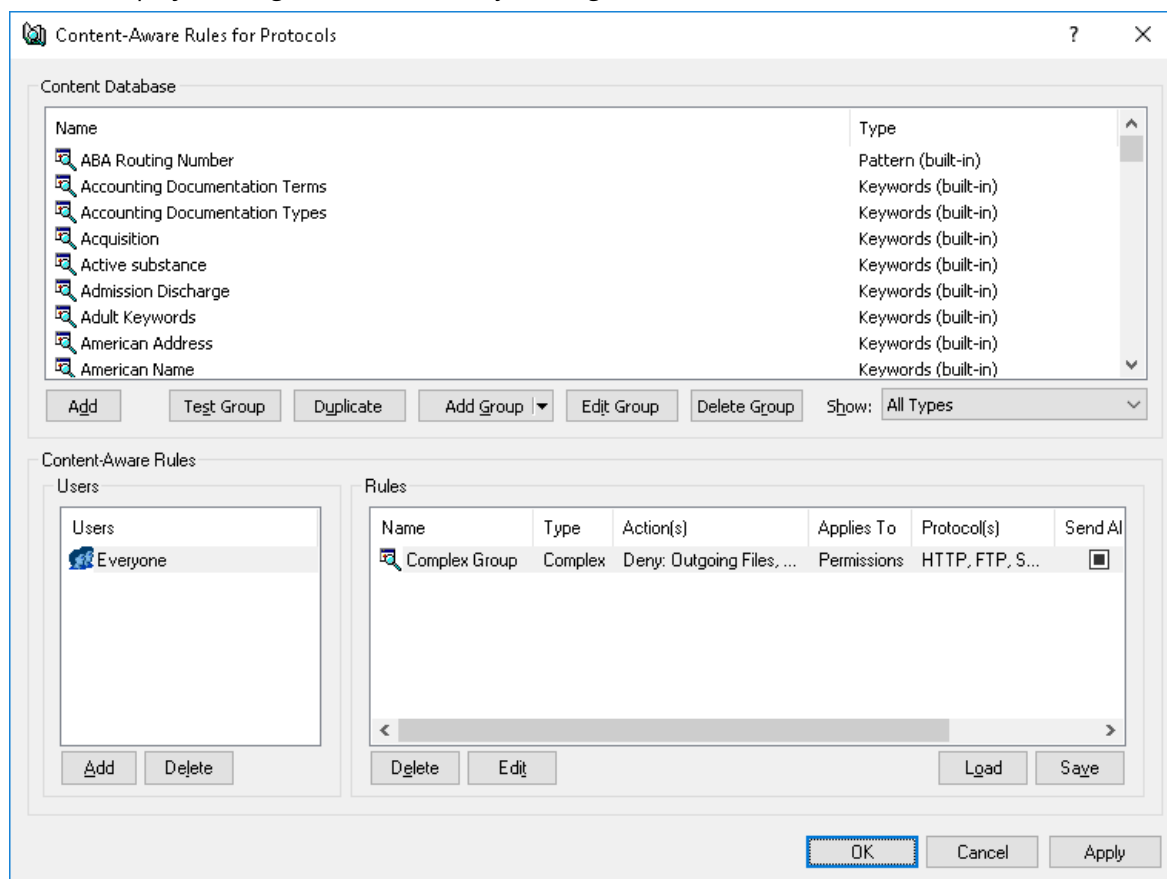
One can define Content-Aware Rules based on custom content groups if the predefined content groups included with DeviceLock do not meet requirements. Custom Pattern content groups enable administrators to specify any character pattern to use to identify sensitive information within text data.

### ***To create a custom Pattern group***

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.

- c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
  - a. Open Group Policy Object Editor.
- d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand either the **Devices** or **Protocols** node.
3. Under the **Devices** or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.

*This will display a dialog box similar to the following.*



4. In the upper pane of the dialog box that appears, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Pattern**.

*This will display the Add Pattern Group dialog box.*

**Add Pattern Group**

Name:

Description:

Expression:

Validation:

Condition:

☒ Case sensitive ☐ Visual anti-spoofing

☒ Cyrillic transliteration

☐ OCR

NOTE: Selection of multiple languages marked with an asterisk (\*) or singular asterisk-marked selections combined with any selection of unmarked languages may cause a performance degradation of the OCR processing engine.

☐ Count identical matches as one match

Test sample:

5. In the **Add Pattern Group** dialog box, do the following:
  - **Name** - Specify the name of the group.
  - **Description** - Specify a description for the group.
  - **Expression** - Set a pattern by specifying one or more Perl regular expressions, one expression per line. The group detects a match in case of a match to any of the expressions specified. For details on regular expressions, refer to the tutorials at [perldoc.perl.org/perlrequick.html](http://perldoc.perl.org/perlrequick.html) and [perldoc.perl.org/perlretut.html](http://perldoc.perl.org/perlretut.html).
  - **Validate** - Check regular expression syntax.
  - **Validation** - When configured to perform validation, the group detects a match only in case of a match to the selected validation type in addition to the expression specified. To match the group, data needs to match the expression and additionally pass the validation. If **No validation** is selected in this field, the group does not perform validation. To match the group in this case, data only needs to match the expression specified.

To configure validation, select the desired type from the drop-down list in this field. The following types of validation are available: **ABA Routing Number, American Name (Ex), Austria SSN, Bulgarian EGN, Canadian Social Insurance Number, China National ID, Credit Card Dump, Credit Card Number (All), Credit Card Number (American Express), Credit Card Number (Diners Club Carte Blanche), Credit Card Number (Diners Club En Route), Credit Card Number (Diners Club), Credit Card Number (Discover), Credit Card Number (JCB), Credit Card Number (Laser), Credit Card Number (Maestro), Credit Card Number (Master Card), Credit Card Number (MIR), Credit Card Number (Solo), Credit Card Number (Switch), Credit Card Number (Visa Electron), Credit Card Number (Visa), Danish Personal ID, Date, Date (ISO), Dominican Republic ID, Email Address, European VAT Number, Finnish ID, France INSEE Code, German eTIN, Health Insurance Claim, IBAN, IP Address, Irish PPSN, Japan: Social Security and Tax Number System, LUHN Checksum, Mexican Tax Id Number, Norwegian Birth Number, NPI, Polish ID, Polish National Identity Card, Quebec Healthcare Medical Number, Russian Bank Account Number, Russian classification of enterprises and organizations, Russian Correspondent Account, Russian Health Insurance Number, Russian KPP, Russian main state registration number, Russian OGRN, Russian OGRNIP, Russian OKATO, Russian OKFS, Russian OKOGU, Russian OKOPF, Russian Passport Issuer Department Code, Russian Pension Insurance Number, Russian Social Card Number, Russian Taxpayer Identification Number, South African Id Number, South Korean Resident Registration Number, Spanish NIF, Taiwan ID, Turkish Id Number, UK National Insurance Number, UK NHS Number, UK Phone Number, UK Post Code, UK Tax Code, URL, US Social Security Number.**

- **Condition** - Select a condition for triggering content inspection rules that employ this group:
  - **Less than or =** - The rule is triggered if the number of matches to the regular expression is no more than the specified number.
  - **Equal to** - The rule is triggered if the number of matches to the regular expression is equal to the specified number.
  - **Greater than or =** - The rule is triggered if the number of matches to the regular expression is no less than the specified number.
  - **Between** - The rule is triggered if the number of matches to the regular expression is within the specified range.
  - **Exact match** - The rule is triggered if the regular expression matches the entire content provided for inspection.

---

### Important

The group checks for an exact match no more than the first megabyte of the content provided for inspection. If the content exceeds 1 MB, the rule with the **Exact match** condition is not triggered even if the first megabyte of the content matches the group's regular expression.

---



---

**Note**

When the **Exact match** condition is selected, the group detects a match if its regular expression matches the whole content being inspected. As a result, the rule is triggered only if the regular expression matches the entire sequence of characters that make up the given content.

With any condition other than **Exact match**, the group searches for a character sequence that matches the given regular expression. A match is detected if somewhere in the content being inspected there is a character sequence matching that expression.

---

- **Case sensitive** - When this check box is selected, the group distinguishes between lowercase and uppercase characters. For example, the words Term and term will be treated differently, so the group can be configured to match the word Term but not term.

When this check box is cleared, the group does not differentiate between uppercase and lowercase characters. For instance, if Term matches the group, then term or even tErM will match it as well.

- **Visual anti-spoofing** - When this check box is selected, the group identifies data matching its expression even if certain data characters are replaced with other ones similar in appearance or meaning, including:
  - Latin characters in the Russian text (such as Latin b in place of Russian б)
  - Latin characters in place of certain numerals (such as Latin s in place of digit 5)
  - Russian characters in the English text (such as Russian n in place of Latin n)
  - Russian characters in place of certain numerals (such as Russian 3 in place of digit 3)
  - Certain symbols in place of Russian characters (such as \* (asterisk) in place of Russian ж)
  - Numerals in place of certain Latin or Russian characters (such as digit 1 in place of Latin I or digit 4 in place of Russian Ч)
  - Arabic-Indic (Eastern Arabic) numerals in place of normal Arabic numerals (such as symbol ٣ in place of digit 3 or symbol ٨ in place of digit 8)

When this check box is cleared, the group strictly distinguishes characters regardless of whether or not they are similar in appearance or meaning.

- **Cyrillic transliteration** - When this check box is selected, the group recognizes Cyrillic text to be detected regardless of whether the text is written in Cyrillic or Latin letters. For example, if the Russian word Серия matches the group, then the word Seriya will match it as well. When this check box is cleared, the match of the text to the group strictly depends upon the alphabet used to spell the text. For example, the group can be configured to match the word Серия but not Seriya.
- **OCR** - Extract text from images for further checking against the regular expression defined in this content group. To do so, select the **OCR** check box and up to 8 languages.

---

**Note**

Selection of multiple Asian languages (marked with an asterisk (\*) in the GUI) or singular Asian language selections combined with any selection of non-Asian languages may cause a performance degradation of the OCR processing engine.

---

For optimal performance and recognition quality, we recommend selecting only those languages that are really needed.

- **Count identical matches as one match** - Combine duplicate matches returned by the regular expression into a single match. To do so, select the **Count identical matches as one match** check box.
  - **Advanced** - Quickly test the regular expression pattern on sample data. Click **Advanced** to display or hide the **Test sample** box.
  - **Test sample** - Enter a test string and view the result. DeviceLock supports real-time color highlighting of test results. All matches are highlighted in green, while strings that do not match the pattern are highlighted in red.
6. Click **OK** to close the **Add Pattern Group** dialog box.
- The new content group created is added to the existing list of content groups under Content Database in the upper pane of the dialog box for managing content-aware rules.*

## Document Properties Content Groups

Document Properties groups are intended to control access to files based on file properties such as file name, size, etc. They can also be used to control access to password-protected documents and archives, and to images containing text.

---

### Note


The AND logic is applied to all file properties specified within a Document Properties group. For example, to control access to files larger than 5 MB in size and password-protected documents and archives, create two separate Document Properties groups: one group for files larger than 5 MB in size and another group for password-protected documents and archives. If these file properties are specified within the same Document Properties group and then Content-Aware Rule based on this content group is created, this rule will only control password-protected documents and archives that are larger than 5 MB.

---

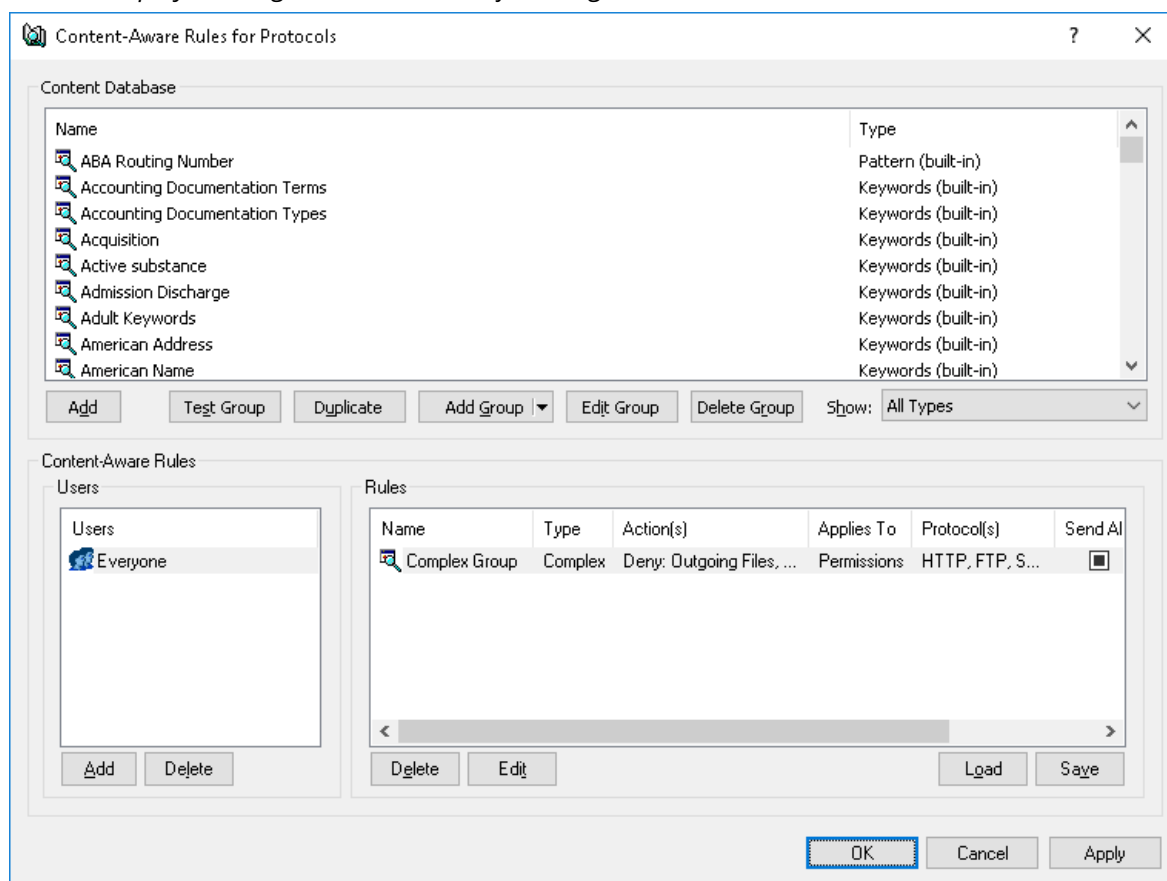
There are no predefined (built-in) Document Properties content groups to use. The following procedure describes how to create custom Document Properties groups.

### **To create a Document Properties group**

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand either the **Devices** or **Protocols** node.
3. Under the **Devices** or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.
  - OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.

*This will display a dialog box similar to the following.*



4. In the upper pane of the dialog box that appears, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Document Properties**.

*This will display the Add Document Properties Group dialog box.*

**Add Document Properties Group**

**Name:**

**Description:**

**Properties**

**File name:**

**Modified:** Not specified 1/ 1/2020 12:00 PM 1/ 1/2020 12:01 PM

**File size:** Not specified 0 0 bytes

☐ Password protected

☐ Text extraction not supported

☐ Contains text 0 %

**Accessed by process:**

**Additional Parameters >>**

**Details**

**Title:**  **Comments:**

**Subject:**  **Authors:**

**Tags:**  **Categories:**

**Company:**  **Last saved by:**

**Manager:**

**Custom & classification fields:**

**Local sender ID(s):**  **Remote recipient ID(s):**

**Local sender E-mail(s):**  **Remote recipient E-mail(s):**

**OK** **Cancel**

5. In the **Add Document Properties Group** dialog box, do the following:
  - **Name** - Specify the name of the group.
  - **Description** - Specify a description for the group.
  - **File name** - Specify the file names. Wildcards, such as \* and ? can be used. An asterisk (\*) matches any series of characters or no characters. For example, \*.txt matches any file name with the extension of txt. The question mark (?) matches any single character. For example, ????.\* matches any file name composed of 4 characters and any extension. Multiple file names must be separated by a semicolon (;), for example, \*.doc; \*.docx.
  - **Modified** - Specify the last modification date/time of the file. To do so, in the **Modified** list, click any of the following options:

- **Not specified** - The last modification date/time is disregarded during content analysis. This option is selected by default.
- **Before than** - The last modification date/time must be earlier than the specified date/time.
- **After than** - The last modification date/time must be later than the specified date/time.
- **Between** - The last modification date/time must fall within the specified date/time range.
- **Not older than** - The last modification date/time must not be older than the specified number of seconds, minutes, hours, days, weeks, months, or years.
- **Older than** - The last modification date/time must be older than the specified number of seconds, minutes, hours, days, weeks, months, or years.

---

### Note

The **Modified** options do not apply to files transmitted over the network. In this case, the last modification date/time is disregarded during content analysis.

---

- **File size** - Specify the file size in bytes, kilobytes, megabytes, gigabytes or terabytes. To do so, in the **File size** list, click any of the following options:
  - **Not specified** - The file's size is disregarded during content analysis. This option is selected by default.
  - **Equal to** - The file's size must be equal to the value specified.
  - **Less than** - The file's size must be less than the value specified.
  - **More than** - The file's size must be more than the value specified.
  - **Between** - The file's size must fall within the specified range of values.

- **Password protected** - Enables the group to detect and control password-protected archives, PDF files, Microsoft Office documents (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx), and AutoCAD 2012 documents (.dwg files).

When a group has the **Password protected** check box selected, rules based on that group detect and control archives and other supported file types where a password is used to restrict access to the file and/or the file's contents. For a list of the supported archive types, see the [Inspection of files within archives](#) feature description.

With Content-Aware Rules, it is considered that a file is password-protected in the following cases only:

- A password is required to open the given file.
- A password is required to access some attachments within the given file.
- The given file includes other password-protected files.

In the latter two cases, the [Archives content inspection on read](#) or [Archives content inspection on write](#) setting must be enabled. Otherwise, in those cases DeviceLock will not consider the given file to be password-protected.

The rules based on the group that has the **Password protected** check box cleared do not account for password-protection of files being inspected.

---

**Note**

An “allow” rule based on a group that has the **Password protected** check box selected takes precedence over “deny” rules (if any), and will allow the transfer of any matching content. An “allow” rule based on a complex group takes precedence in a situation where the logically connected chain of groups that allows the given content includes a group with the **Password protected** check box selected.

---

- **Text extraction not supported** - Control access to unsupported file formats. If this check box for a Document Properties group is selected, and then a Content-Aware Rule based on this content group is created, this rule will control access to all files in an unsupported format. All supported file formats are listed in the [ContentLock and NetworkLock](#) section (see [Expansive coverage of multiple file formats and data types](#)). This parameter can be used to allow transfer of split (or multi-volume) .cab or .rar archives that by default cannot be unpacked and analyzed in case there are active content-aware rules combined with **Archives content inspection on read** or **Archives content inspection on write** options enabled in **Service options**. “Allow” Content-Aware Rules based on Document Properties group with the **Text extraction not supported** flag enabled take precedence over deny rules and allow the transfer of any matching content, including the transfer of split (or multi-volume) archives.
- **Contains text** - Detect and control access to images based on whether or not they contain text. If the **Contains text** check box for a Document Properties group is selected, and then a complex Content-Aware Rule is created based on this content group and the **Images, CAD & Drawing** built-in content group (File Type Detection) combined by AND logic, this rule will check whether supported image files contain text and control access to text images. Clear the **Contains text** check box if it is not desired to detect and control access to text images. For information on the supported image file types, see the [Text in picture detection](#) feature description. Having selected the **Contains text** check box, specify the amount of text that images must contain. The amount of text is expressed as a percentage of the total image area. For example, if text occupies ½ of the image, the amount of text makes 50%. If an image contains only text, the amount of text is 100%.

---

**Note**

The **Contains text** parameter also applies to other supported file formats (see [Expansive coverage of multiple file formats and data types](#)). In this case, the percentage refers to the ratio of the text size in characters to file size in bytes.

---

- **Accessed by process** - Specify the name of the process accessing the document’s file. Wildcards, such as asterisks (\*) and question marks (?), can be used. Multiple process names must be separated by a semicolon (;), for example, explorer.exe; notepad.exe.
- **Additional Parameters** - Configure the group to recognize various properties of inspected documents, such as built-in and custom properties of Microsoft Office documents and other document types, senders and recipients of instant messages and emails, and classification

labels applied by third-party products like Boldon James Classifier.

When using additional parameters, consider the following:

- Different parameters are combined by AND logic, that is, the group recognizes a document if it matches each of the parameters configured. Thus, for a document to be recognized by a group that has the Title and Subject parameter values specified, both the Title and Subject properties of the document must have the respective values. If it is required to combine parameters by OR logic, one could configure a Complex group by adding to it a separate Document Properties group for each parameter.
- It is possible to specify multiple values for the same parameter by separating them with a semicolon. In this case, the values are combined by OR logic, so that the group recognizes a document if it matches any of the values specified. Thus, if Report; Account is specified in the Title parameter, then the group recognizes documents that have the Title property value of Report OR Account.

The following additional parameters are available:

- **Title, Subject, Tags, Company, Manager, Comments, Authors, Categories, Last saved by** - These fields are used to enter values matching some frequently used properties of documents subjected to control. Supported are properties of MS Office documents (.docx, .xlsx, .pptx, .vsdx), .pdf, and compound documents. The title of the field corresponds to the property name specified in document management applications such as MS Office Word or Adobe Acrobat.

Each field allows the use of wildcards: an asterisk (\*) denotes any group of characters or no characters; a question mark (?) denotes a single arbitrary character. In a field, multiple values can be entered by separating them with a semicolon (;). Example of entering two values with wildcards: \*Report\*; \*Account\*.

Values entered in different fields are combined by AND logic. If multiple values are entered in the same field, they are combined by OR logic.

- **Custom & classification fields** - This field can be used to enter values matching built-in or custom properties of documents subjected to control. Supported are properties of MS Office documents (.docx, .xlsx, .pptx), .pdf and compound documents.

To enter a single value for some property, use the following syntax:

<property name>=<property value>. Thus, Division=Sales represents the value of Sales for the Division property. To enter multiple values for the same property, separate them with a comma. In this case, values are combined by OR logic. Thus, Division=Sales,Finance represents the value of Sales OR Finance for the Division property.

To enter values for multiple properties, separate property entries by a semicolon, such as <name1>=<value11>,<value12>; <name2>=<value21>. Values of different properties are combined by AND logic while different values of the same property are combined by OR logic. Thus, Division=Sales,Finance; Office=Head Office represents the value of Sales OR Finance for the Division property AND the value of Head Office for the Office property.

By using the **Custom & classification fields** box, the group can also be configured to recognize classification labels of third-party products like Boldon James Classifier that save their label values in document properties. If the label is the exact value of some property,

then, to recognize it, one can use the syntax described above:

<property name>=<property value>. The value of whichever property of the document serves for the designation of the label is determined by the settings of the third-party product.

To set up the group to recognize Boldon James Classifier's SISL labels, a syntax is used that indicates the ID of the uid element of the desired label: uid=<ID value>. The ID value can be found from the XML data of the SISL label stamped on a document classified. For further details, see [Recognizing Boldon James Classifier Labels](#).

In the **Custom & classification fields** box, a semicolon (;) can be used as a separator to enter more than one entry designating document properties and/or classification labels. All semicolon-separated entries are combined by AND logic.

---

#### Note

To assist with configuring the group, the **Custom & classification fields** box stores previous entries and provides them for selection from the drop-down list supplementing this box.

---

- **Local sender ID(s), Remote recipient ID(s)** - These fields are used to enter identifiers of local users sending and/or identifiers of remote users receiving instant messages subjected to control. Separate identifiers with a comma (,) or semicolon (;). Use wildcards (\* and ?) as may be required.

---

#### Note

Local sender ID(s) and Remote recipient ID(s) apply only to protocols. In content-aware rules for devices these parameters have no effect.

---

User identifiers can be specified for the following protocols: ICQ Messenger, Jabber, Mail.ru Agent, Skype, Telegram, Viber, WhatsApp, Zoom.

ICQ Messenger users are identified by UIN number (such as 23232323).

Jabber users are identified by Jabber ID in the following format: <user>@<domain>.

Mail.ru Agent users are identified by email address in the following format: <user>@mail.ru.

Skype, Telegram, Viber, WhatsApp, and Zoom users are identified by user ID.

- **Local sender E-mail(s), Remote recipient E-mail(s)** - These fields are used to enter addresses of local users sending and/or addresses of remote users receiving emails subjected to control. Separate addresses with a comma (,) or semicolon (;). Use wildcards (\* and ?) as may be required.

---

#### Note

Local sender E-mail(s) and Remote recipient E-mail(s) apply only to protocols. In content-aware rules for devices these parameters have no effect.

---

Email addresses can be specified for the following protocols: MAPI, SMTP, IBM Notes, Web Mail.

Use the following format for an email address: <user>@<domain> (or <user>/<domain> for IBM Notes). An asterisk (\*) can be used to specify a group of addresses. For example, \*@domain.com (or \*/domain for IBM Notes) identifies all email addresses in the specified domain.



When using these parameters in the case of Web Mail, take into account the following:

- Since the sender and recipient cannot be checked during upload of attachments to the Web server, we do not recommend the use of these parameters in the content security policies for Web Mail users. For security reasons, DeviceLock does not allow uploading attachments to the Web server if the rule that allows sending attachments via Web Mail employs Local sender E-mail(s) or Remote recipient E-mail(s).
- Rules that control sending emails via Web Mail allow saving draft messages that do not specify restricted senders or recipients, which may enable unauthorized persons to access the content you want to protect. For this reason, using such a rule is not advisable.

When using parameters to designate senders or recipients, consider the following:

- To allow or deny the transfer of particular content between specific persons, we recommend the use of Complex content groups where a Document Properties group that specifies the desired senders and/or recipients is combined by AND logic with other content groups (File Type Detection, Keywords, etc.).

6. Click **OK** to close the **Add Document Properties Group** dialog box.

*The new content group created is added to the existing list of content groups under Content Database in the upper pane of the dialog box for managing content-aware rules.*

## Recognizing Boldon James Classifier Labels

Document Properties groups allow for content inspection using labels that Boldon James Classifier applications stamp on documents. One can implement this by configuring a group to recognize desired labels and then creating content-aware rules based on that groups. The rules can be applied to both devices and network protocols, thus enabling the use of Boldon James Classifier labels to control content access/sending permissions, content-aware shadowing, and/or simple content detection.

For MS Office documents, Boldon James Classifier stores its labels in document properties. When a document is stamped with a label, a number of new properties containing the label data are added to the document. These properties and their values can be explored in the standard dialog box for viewing document properties in MS Office applications. Most of those properties have the bj prefix at the beginning of their name.

A label can be the exact value of a document property, such as bjDocumentSecurityLabel: This information is Classified | Internal. To set up the group to recognize a label like this, one should apply the syntax <property name>=<property value> in the **Custom & classification fields** box (see [description of that box](#) in the topic [Document Properties Content Groups](#)).

Boldon James Classifier can also represent its labels in the form of XML data held in document properties. Labels of this kind are referred to as SISL labels. For MS Office documents, SISL label data is stored in the property named bjDocumentLabelXML. A part of the label's XML data string can be stored in the supplemental property bjDocumentLabelXML-0.

The SISL label value is the ID of the uid element in the label's XML data. The ID can be a string or numeric value. To set up the group to recognize such a label, one should apply the syntax that

indicates the ID of the uid element of the SISL label: uid=<ID value> (see description of the [Custom & classification fields](#) box in the topic [Document Properties Content Groups](#)).

For example, in the bjDocumentLabelXML property of an MS Office document you might encounter the following SISL label data:

```
<?xml version="1.0" encoding="us-ascii"?><sisl
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xmlns:xsd="http://www.w3.org/2001/XMLSchema" sislVersion="0"
policy="b669e953-f8eb-49a8-a8f3-ffec153ba63e"
xmlns="http://www.boldonjames.com/2008/01/sie/internal/label"><element
uid="id_classification_internalonly" value="" /></sisl>
```

To recognize this label, specify the following entry in the **Custom & classification fields** box:  
uid=id\_classification\_internalonly (without quotes).

## Complex Content Groups

Complex groups allow the use of Boolean expressions for a more flexible definition of the data to be controlled. These groups can include any combination of built-in or custom content groups (File Type Detection, Keywords, Pattern, Document Properties, Digital Fingerprints) linked by standard logical operators. Each content group is treated as a single filter criterion that can be included in the Boolean expression. Combining multiple content groups in a Complex content group enables the creation of complex filters to identify sensitive content of data transmitted over the network.

The following table lists the logical operators in order of precedence from highest to lowest.


Operator	Meaning
NOT	Logical negation of a filter criterion
AND	Both filter criteria must apply
OR	Either filter criterion can apply

Parentheses can be used to modify the precedence of operators and force some parts of an expression to be evaluated before others. Nested criteria enclosed in parentheses are evaluated in inner-to-outer order. Multiple levels of nesting are supported. A Complex group can contain a maximum of 50 content groups.

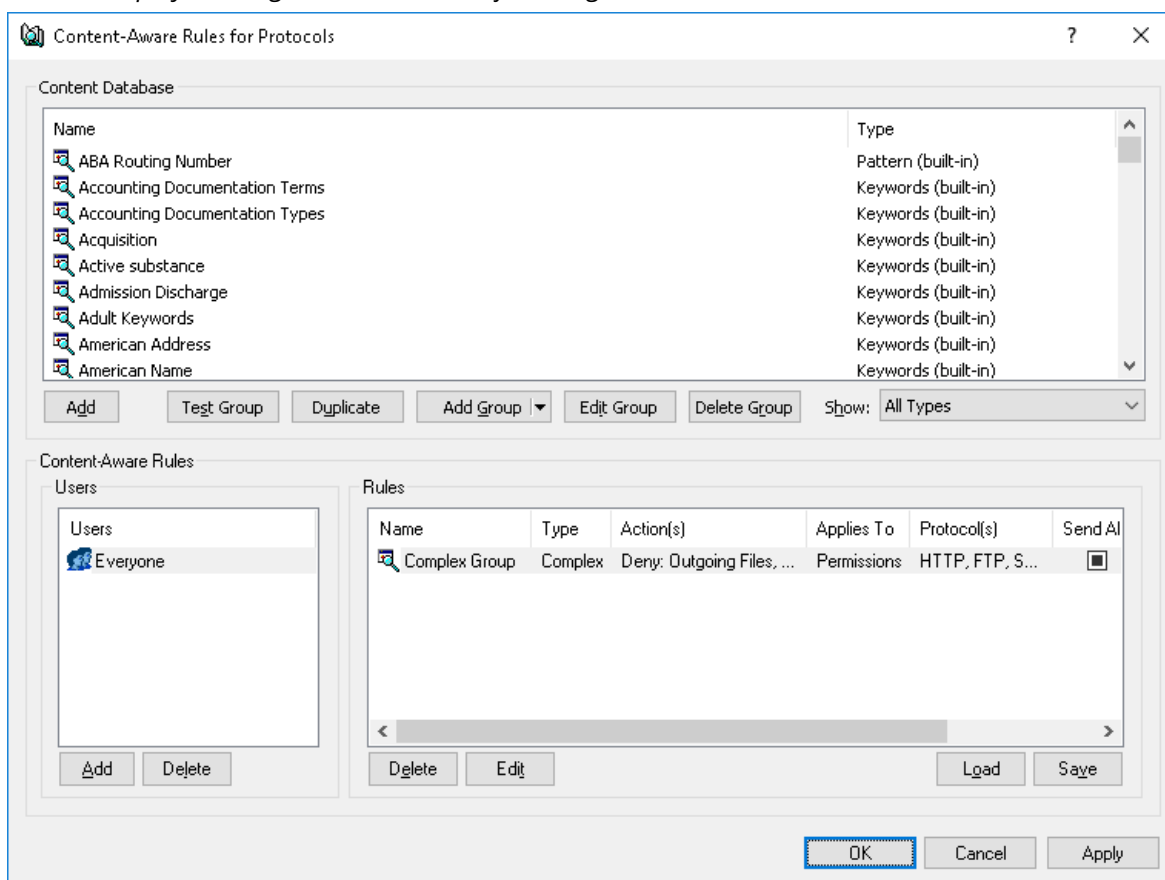
There are no predefined (built-in) Complex content groups to use. The following procedure describes how to create custom Complex groups.

### ***To create a Complex group***

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:

- a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand either the **Devices** or **Protocols** node.
  3. Under the **Devices** or **Protocols** node, do one of the following:
    - Right-click **Content-Aware Rules**, and then click **Manage**.
    - OR -
    - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.

*This will display a dialog box similar to the following.*



4. In the upper pane of the dialog box that appears, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Complex**.  
*This will display the Add Complex Group dialog box.*

**Add Complex Group**

Name:

Description:

NOT	(	Criteria	)	AND/OR

Result

5. In the **Add Complex Group** dialog box, do the following:
  - **Name** - Specify the name of the group.
  - **Description** - Specify a description for the group.
  - **Add** - Add content groups from the Content Database to the end of the group list in the **Criteria** column:
    - a. Click **Add**, or double-click a blank area in the **Criteria** column.
    - b. In the dialog box that appears, select the content group, and then click **OK**, or double-click the content group.  
*You can select multiple content groups by holding down the SHIFT key or the CTRL key while clicking them.*  
*To view information about a content group, select the desired group, and then click View Group.*  
*The content groups added appear in the Criteria column in the Add Complex group dialog box.*  
*Each content group added is treated as a single filter criterion that can be included in the Boolean expression.*
  - **Insert** - Add a content group from the Content Database above the group selected in the **Criteria** column:
    - a. Select a group in the **Criteria** column, and then click **Insert**.
    - b. In the dialog box that appears, select the content group to insert, and then click **OK**, or double-click the content group to insert.

- **View** - View information about the group selected in the **Criteria** column:
    - Select a group in the **Criteria** column, and then click **View**, or double-click the group to view.
  - **Delete** - Delete the selected group from the **Criteria** column.
  - **NOT** - Apply the logical NOT operator to each of the selected content groups. To do so, select the desired group in the **Criteria** column, and then select the appropriate check box in the **NOT** column.
  - **AND/OR** - Join each of the selected content groups with the logical AND or OR operator. To do so, select the desired group in the **Criteria** column, and then click either **AND** or **OR** in the appropriate list in the **AND/OR** column.
  - **Clear** - Clear the current list of content groups in the **Criteria** column.
  - **Validate** - Validate the expression. If the expression was defined incorrectly (for example, an opening parenthesis was not matched with a closing parenthesis), an error message will appear.
6. Click **OK** to close the **Add Complex Group** dialog box.
- The new content group created is added to the existing list of content groups under Content Database in the upper pane of the dialog box for managing content-aware rules.*

---

#### Note

When moving an entry to the place of an adjacent one in the list of groups, the **NOT** check box setting moves together with the entry if the number of opening brackets is less than or equal to that of closing ones both in the moved entry and in the entry to which place it is moved. If at least one of them has more opening brackets than closing ones, the **NOT** check box setting does not move to the adjacent entry. Such a solution helps preserve the logical structure of the expression when the order of the list entries changes.


---

## Viewing Built-in Content Groups

It is possible to view any built-in content groups, but they cannot be modified or deleted.

### **To view a built-in content group**


1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand either the **Devices** or **Protocols** node.

3. Under the **Devices** or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.  
- OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.  
*This will display a dialog box for managing content-aware rules.*
4. In the upper pane of the dialog box that appears, under **Content Database**, select any built-in group to view, and then click **View Group**.

## Duplicating Built-in Content Groups

While editing the built-in content groups is not allowed, it is possible to create and use their editable copies (duplicates) to suit a particular organization's needs.


### ***To duplicate a built-in content group***

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand either the **Devices** or **Protocols** node.
3. Under the **Devices** or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.  
- OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.  
*This will display a dialog box for managing content-aware rules.*
4. In the upper pane of the dialog box that appears, under **Content Database**, select any built-in group to duplicate it, and then click **Duplicate**.
5. In the dialog box that opens, edit the content group as required, and then click **OK**.  
*The new content group created is added to the existing list of content groups under Content Database in the upper pane of the dialog box for managing content-aware rules.*

## Editing or Deleting Custom Content Groups

Custom content groups can be modified or deleted as needed.

### ***To edit or delete a custom content group***

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand either the **Devices** or **Protocols** node.
3. Under the **Devices** or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.
  - OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.


*This will display a dialog box for managing content-aware rules.*
4. In the upper pane of the dialog box that appears, under **Content Database**, select any custom group to edit or delete.
5. Click **Edit Group** to modify the selected content group. In the dialog box that opens, make the required changes, and then click **OK**.  
- OR -  
Click **Delete Group** or press the DELETE key to delete the selected content group.
6. In the dialog box for managing content-aware rules, click **OK** or **Apply** to apply the changes.

## Testing Content Groups

It is possible to test any built-in or custom content group by checking to see whether specified files match with it. These tests can be used to verify that the rules that are created based on the content groups meet a specific business requirement.

### **To test a content group**

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand either the **Devices** or **Protocols** node.

3. Under the **Devices** or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.  
- OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.
4. In the upper pane of the dialog box that appears, under **Content Database**, select the content group to test, and then click **Test Group**.  
*Only one group can be tested at a time.*
5. In the **Open** dialog box that appears, locate and select a probe file to use for testing the content group, and then click **Open**.  
When testing a Digital Fingerprints group, the DeviceLock Enterprise Server is required to check the fingerprints of the probe file. Therefore, the console displays a dialog box to specify the DeviceLock Enterprise Server that hosts the digital fingerprints database. To continue the test, enter the name of the computer running the DeviceLock Enterprise Server. For details regarding the fingerprinting technique, see [Digital Fingerprints](#).  
The console preserves the server name specified, and uses it during the console session without repeatedly prompting for a server name. In subsequent sessions, the console displays the dialog box again, allowing a different server to be specified. By default, it chooses the server that was used in the previous session.

Once the processing of the probe file has been complete, a message box appears with the test result. If the file meets the conditions of the content group, the message box displays the following message: "Selected file matches with the group." Otherwise, the following message is displayed: "Selected file does not match with the group."

---

**Note**

While testing is in progress, the console stops responding (hangs).

---

## Managing Content-Aware Rules

Managing Content-Aware Rules involves the following tasks:

- [Defining Content-Aware Rules](#)
- [Editing Content-Aware Rules](#)
- [Copying Content-Aware Rules](#)
- [Exporting and Importing Content-Aware Rules](#)
- [Undefining Content-Aware Rules](#)
- [Deleting Content-Aware Rules](#)

Content-Aware Rules can be managed using DeviceLock Management Console, DeviceLock Group Policy Manager, or the DeviceLock Service Settings Editor.

## Defining Content-Aware Rules

Content-Aware Rules are created based on either the built-in or custom content groups. For detailed information on these groups, see [Configuring Content Groups](#).



It is possible to enable alerts that are sent when a specific Content-Aware Rule fires. Such alerts are enabled when defining a Content-Aware Rule.


DeviceLock sends alerts based on the alerting settings. These settings specify where and how the alerts should be sent. Prior to enabling alerts for a specific Content-Aware Rule, alerting settings must be configured in DeviceLock Service options (see [Alerts](#)).

This section covers:

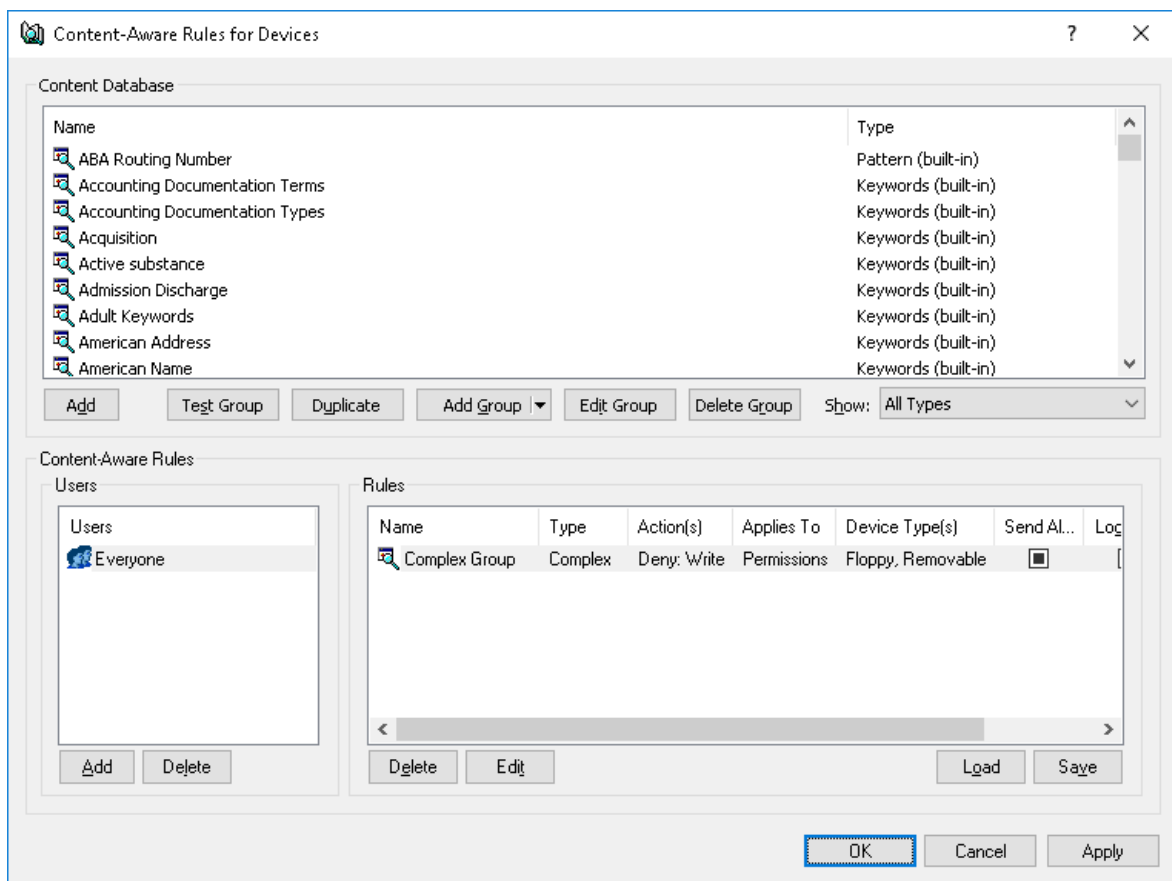
- [Defining Rules for Devices](#)
- [Defining Rules for Protocols](#)

## Defining Rules for Devices

Use the following steps to define a Content-Aware Rule for devices:

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand the **Devices** node.
3. Under the **Devices** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.
  - OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.

*This will display a dialog box similar to the following.*



4. In the lower-left pane of the dialog box that appears, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which to define the rule, and then click **OK**.  
*The users and groups added are displayed under Users in the lower-left pane of the dialog box for managing content-aware rules.*  
 To delete a user or group, in the lower-left pane of the dialog box for managing rules, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.
6. In the lower-left pane of the dialog box for managing rules, under **Users**, select the users or groups for which the rule should apply.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
7. In the upper pane of the dialog box for managing rules, under **Content Database**, select the desired content group, and then click **Add**, or double-click the desired content group.

---

#### Note

Only one content group can be specified for a Content-Aware Rule.

---

*The Add Rule dialog box appears.*

**Add Rule**

Name:

Applies to

☐ Permissions ☐ Shadowing ☐ Detection

If this rule triggers

☐ Send Alert ☐ Log Event ☐ Shadow Copy

Devices Type(s):

Actions

	Allow	Deny
User's Rights		

View Group OK Cancel

8. In the **Add Rule** dialog box, in the **Name** box, type the name of the Content-Aware Rule. By default, the rule has the same name as its content group. The name of the rule can be changed if needed.

To view this rule's content group, click the **View Group** button in the bottom left corner of the dialog box. The console displays the properties of the group in a separate dialog box, allowing property values to be viewed but not modified.

9. Under **Applies to**, specify the type of operation associated with the rule. The available options are:
  - **Permissions** - Specifies that the rule will apply to access control operations.
  - **Shadowing** - Specifies that the rule will apply to shadow copy operations.
  - **Detection** - Specifies that the rule will detect specified content in transferred data, log detection events, and send alerts to the administrator if the appropriate flags have been set.
  - **Permissions, Shadowing** - Specifies that the rule will apply to both access control and shadow copy operations.
  - **Permissions, Detection** - Specifies that the rule will apply to both access control and detection operations.

- **Shadowing, Detection** - Specifies that the rule will apply to both shadow copy and detection operations.
- **Permissions, Shadowing, Detection** - Specifies that the rule will apply to both access control and shadow copy operations, as well as to detection operations.

---

#### Note

To successfully create/save a rule that applies either to detection operations only or to detection operations combined with other operations, at least one of the following options must be selected for this rule: **Log Event**, **Send Alert** or **Shadow Copy** (see step 10 of this procedure). Otherwise, the rule cannot be saved and the following message appears: "Log Event, Send Alert or Shadow Copy should be specified."

---

- Under **If this rule triggers**, specify the following additional actions to be performed when the rule triggers:

- **Send Alert** - Specifies that an alert is sent whenever the rule triggers.
- **Log Event** - Specifies that an event is logged in the Audit Log whenever the rule triggers.
- **Shadow Copy** - Specifies that a shadow copy of data is created whenever the rule triggers.

When alerts, audit and/or shadowing are enabled or disabled in a Content-Aware Rule, the rule setting takes precedence over the respective setting for the device type.

Example: If audit is enabled for a particular device type and disabled in a rule for that device type, the triggering of the rule does not cause audit events. If audit is enabled in the rule, then the triggering of the rule causes audit events, even if audit is disabled at the device-type level.

The rule can also inherit the alert, audit and/or shadowing setting from the device-type level. This is the default option, represented by the indeterminate state of the check boxes (neither checked nor cleared). The state of each check box can be changed individually.

Example: When a rule inherits the audit setting from the device-type level, the triggering of the rule causes audit events only if audit is enabled for the device type controlled by that rule.

- Under **Device Type(s)**, select the appropriate device type(s) for this rule to be applied to.

*Content-Aware Rules can be applied to the following device types: Clipboard, Floppy, iPhone, MTP, Optical Drive, Palm, Printer, Removable, TS Devices, and Windows Mobile.*

*Under Action(s), if you multi-select device types that have different combinations of configurable access rights, the dialog box will display the superset of access rights for the selection list: those that are common to all selected device types, and those that do not necessarily apply to all types. As would be expected, if a particular access right that is displayed is not common to one or more particular selected device types, its setting cannot be applied to those device types and will only apply to types where the setting is supported.*

- Under **Action(s)**, specify which user actions are allowed or disallowed on files, which user actions are logged to the Shadow Log, and in which cases content detection occurs.  
If the rule applies to shadow copy operations combined with other operations, the Read user right becomes unavailable. If the rule applies to detection operations combined with other operations, only the "Allow" action becomes available. For detailed information on user rights and actions that can be specified in Content-Aware Rules, see [Access Control](#), [Content-Aware Shadowing](#) and [Content-Aware Detection](#) for devices.

13. Click **OK**.


*The rule created is displayed under Rules in the lower-right pane of the dialog box for managing content-aware rules.*

14. Click **OK** or **Apply** to apply the rule.

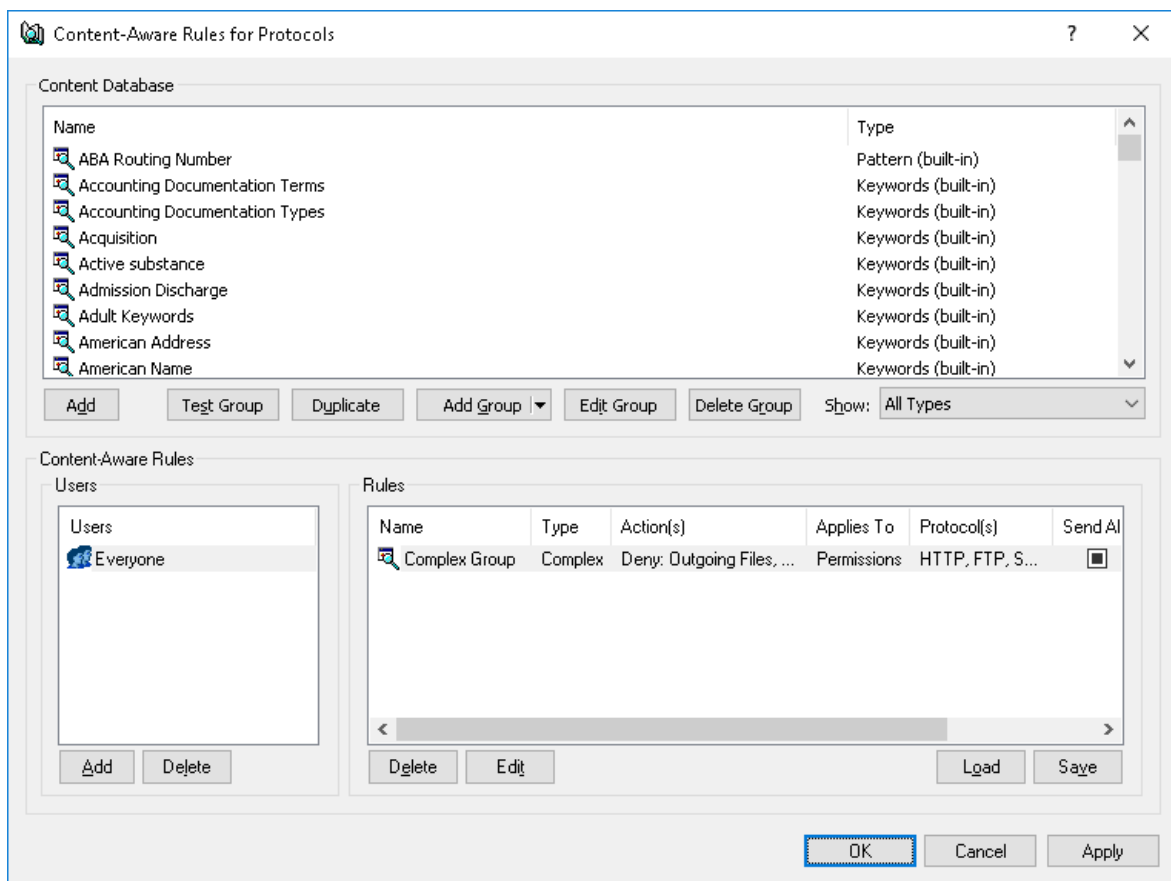
The users or groups to which device-related Content-Aware Rules apply, are displayed under **Devices > Content-Aware Rules** in the console tree. When a user or group is selected to which a Content-Aware Rule applies, the details pane will show detailed information regarding that rule (see [List of Content-Aware Rules for Devices](#)).

## Defining Rules for Protocols

Use the following steps to define a Content-Aware Rule for protocols:

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand the **Protocols** node.
3. Under the **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.  
- OR -
  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.

*This will display a dialog box similar to the following.*



4. In the lower-left pane of the dialog box that appears, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which to define the rule, and then click **OK**.  
*The users and groups added are displayed under Users in the lower-left pane of the dialog box for managing content-aware rules.*  
 To delete a user or group, in the lower-left pane of the dialog box for managing rules, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.
6. In the lower-left pane of the dialog box for managing rules, under **Users**, select the users or groups for which the rule should apply.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
7. In the upper pane of the dialog box for managing rules, under **Content Database**, select the desired content group, and then click **Add**, or double-click the desired content group.

---

### Note

Only one content group can be specified for a Content-Aware Rule.

---

*The Add Rule dialog box appears.*

**Add Rule**

Name:

Applies to: ☐ Permissions ☐ Shadowing ☐ Detection

If this rule triggers: ☐ Send Alert ☐ Log Event ☐ Shadow Copy

Protocol(s):

Actions:

	Allow	Deny
User's Rights		

View Group OK Cancel

8. In the **Add Rule** dialog box, in the **Name** box, type the name of the Content-Aware Rule. By default, the rule has the same name as its content group. The name of the rule can be changed if needed.

To view this rule's content group, click the **View Group** button in the bottom left corner of the dialog box. The console displays the properties of the group in a separate dialog box, allowing property values to be viewed but not modified.

9. Under **Applies to**, specify the type of operation associated with the rule. The available options are:
  - **Permissions** - Specifies that the rule will apply to access control operations.
  - **Shadowing** - Specifies that the rule will apply to shadow copy operations.
  - **Detection** - Specifies that the rule will detect specified content in transferred data, log detection events, and send alerts to the administrator if the appropriate flags have been set.
  - **Permissions, Shadowing** - Specifies that the rule will apply to both access control and shadow copy operations.
  - **Permissions, Detection** - Specifies that the rule will apply to both access control and detection operations.

- **Shadowing, Detection** - Specifies that the rule will apply to both shadow copy and detection operations.
- **Permissions, Shadowing, Detection** - Specifies that the rule will apply to both access control and shadow copy operations, as well as to detection operations.

---

#### Note

To successfully create/save a rule that applies either to detection operations only or to detection operations combined with other operations, at least one of the following options must be selected for this rule: **Log Event**, **Send Alert** or **Shadow Copy** (see Step 10 of this procedure). Otherwise, the rule cannot be saved and the following message appears: "Log Event, Send Alert or Shadow Copy should be specified."

---

- Under **If this rule triggers**, specify the following additional actions to be performed when the rule triggers:

- **Send Alert** - Specifies that an alert is sent whenever the rule triggers.
- **Log Event** - Specifies that an event is logged in the Audit Log whenever the rule triggers.
- **Shadow Copy** - Specifies that a shadow copy of data is created whenever the rule triggers.

When alerts, audit and/or shadowing are enabled or disabled in a Content-Aware Rule, the rule setting takes precedence over the respective setting for the protocol.

Example: If audit is enabled for a particular protocol and disabled in a rule for that protocol, the triggering of the rule does not cause audit events. If audit is enabled in the rule, then the triggering of the rule causes audit events, even if audit is disabled at the protocol level.

The rule can also inherit the alert, audit and/or shadowing setting from the protocol level. This is the default option, represented by the indeterminate state of the check boxes (neither checked nor cleared). The state of each check box can be changed individually.

Example: When a rule inherits the audit setting from the protocol level, the triggering of the rule causes audit events only if audit is enabled for the protocol controlled by that rule.

- Under **Protocol(s)**, select the appropriate protocol(s) for this rule to be applied to.  
*Content-Aware Rules can be applied to the following protocols: Career Search, File Sharing, FTP, HTTP, IBM Notes, ICQ Messenger, IRC, Jabber, Mail.Ru Agent, MAPI, Skype, SMB, SMTP, Social Networks, Telegram, Viber, Web Mail, Web Search, WharsApp, and Zoom.*

*Under Action(s), if you multi-select protocols that have different combinations of configurable access rights, the dialog box will display the superset of access rights for the selection list: those that are common to all selected protocols, and those that do not necessarily apply to all protocols. As would be expected, if a particular access right that is displayed is not common to one or more particular selected protocols, its setting cannot be applied to those protocols and will only apply to protocols where the setting is supported.*

- Under **Action(s)**, specify which user actions are allowed or disallowed on protocols, which user actions are logged to the Shadow Log, and in which cases content detection occurs.  
If the rule applies to shadow copy operations combined with other operations, the Read user right becomes unavailable. If the rule applies to detection operations combined with other operations, only the "Allow" action becomes available. For detailed information on user rights



and actions that can be specified in Content-Aware Rules, see [Access Control](#), [Content-Aware Shadowing](#) and [Content-Aware Detection](#) for protocols.

13. Click **OK**.

*The rule created is displayed under Rules in the lower-right pane of the dialog box for managing content-aware rules.*

14. Click **OK** or **Apply** to apply the rule.

The users or groups to which protocol-related Content-Aware Rules apply, are displayed under **Protocols > Content-Aware Rules** in the console tree. When a user or group is selected to which a Content-Aware Rule applies, the details pane will show detailed information regarding that rule (see [List of Content-Aware Rules for Protocols](#)).

## Editing Content-Aware Rules

By editing a Content-Aware Rule, it is possible to modify the rule properties such as **Name**, **Applies To**, **If this rule triggers**, **Protocol(s)**, **Actions**.

### **To edit a Content-Aware Rule**

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Do one of the following:
  - In the case of a rule for devices, expand the **Devices** node.
  - In the case of a rule for protocols, expand the **Protocols** node.
3. Under the **Devices** node or **Protocols** node, right-click **Content-Aware Rules**, click **Manage**, and then do the following:
  - a. In the lower-left pane of the dialog box that appears, under **Users**, select the user or group for which to edit the rule.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.*
  - b. In the lower-right pane of the dialog box, under **Rules**, select the rule to edit, and then click **Edit**.
    - OR -
    - Right-click the rule, and then click **Edit**.
    - OR -
    - Double-click the rule.

- OR -

Under the **Devices** node or **Protocols** node, expand **Content-Aware Rules**, and then do the following:

- a. Under **Content-Aware Rules**, select the user or group for which to edit the rule.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them in the details pane.*

- c. In the details pane, right-click the rule to edit, and then click **Edit**.

- OR -

In the details pane, double-click the rule to edit.

*The Edit Rule dialog box appears.*

4. In the **Edit Rule** dialog box, modify the rule properties to meet requirements.
5. Click **OK** to apply the changes.


## Copying Content-Aware Rules

It is possible reuse existing Content-Aware Rules by performing a cut-and-paste operation, a copy-and-paste operation, or a drag-and-drop operation.

### **To copy a Content-Aware Rule**

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Do one of the following:
  - In the case of a rule for devices, expand the **Devices** node.
  - In the case of a rule for protocols, expand the **Protocols** node.
3. Under the **Devices** node or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage**.

- OR -

  - Select **Content-Aware Rules**, and then click **Manage**  on the toolbar.

*This will display a dialog box for managing content-aware rules.*

4. In the lower-left pane of the dialog box managing rules, under **Users**, select the user or group to which the rule to copy is applied.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.*



5. In the lower-right pane of the dialog box for managing rules, under **Rules**, right-click the rule to copy, and then click **Copy** or **Cut**.  
*A copy of the rule is automatically placed onto the Clipboard.*  
*You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When CTRL+X is used to cut the rule, the rule will be cut only after it is pasted.*  
*To perform a drag-and-drop operation, select the rule and move it to the user or group to apply the copied rule.*
6. In the lower-left pane of the dialog box for managing rules, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to apply the copied rule, and then click **OK**.  
*The users and groups that are added are displayed under Users in the lower-left pane of the dialog box for managing content-aware rules.*
8. In the lower-left pane of the dialog box for managing rules, under **Users**, select the users or groups to apply the copied rule.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
9. In the lower-right pane of the dialog box for managing rules, right-click in the **Rules** pane and then click **Paste**.  
*The copied rule is displayed under Rules in the lower-right pane of the dialog box for managing content-aware rules.*
10. Click **OK** or **Apply** to apply the copied rule.

## Exporting and Importing Content-Aware Rules

It is possible to export all the current Content-Aware Rules to a **.cwl** file that can later be imported and used on another computer. Exporting and importing can also be used as a form of backup.


### **To export Content-Aware Rules**


1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
 If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
 If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Do one of the following:
  - In the case of rules for devices, expand the **Devices** node.
  - In the case of rules for protocols, expand the **Protocols** node.

3. Under the **Devices** node or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Save**.
    - OR -
  - Select **Content-Aware Rules**, and then click **Save**  on the toolbar.
    - OR -
  - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Save**.
    - OR -
  - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Save**.
    - OR -
  - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Save**  on the toolbar.
    - OR -
  - Right-click **Content-Aware Rules**, and then click **Manage**. In the lower-right pane of the dialog box that appears, under **Rules**, click **Save**.
4. In the **Save As** dialog box that appears, specify the name and location of the .cwl file, and then click **Save**.
 

*The exported rules are saved in a file with a .cwl file name extension.*

### **To import Content-Aware Rules**

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Do one of the following:
  - In the case of rules for devices, expand the **Devices** node.
  - In the case of rules for protocols, expand the **Protocols** node.
3. Under the **Devices** node or **Protocols** node, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Load**.
    - OR -
  - Select **Content-Aware Rules**, and then click **Load**  on the toolbar.
    - OR -
  - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Load**.
    - OR -

- Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Load**.  
- OR -
  - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Load**  on the toolbar.  
- OR -
  - Right-click **Content-Aware Rules**, and then click **Manage**. In the lower-right pane of the dialog box that appears, under **Rules**, click **Load**.
4. In the dialog box that appears, locate and select the file to import, and then click **Open**.  
*Only one .cwl file can be imported at a time.*

## Undefined Content-Aware Rules

When deploying DeviceLock policies with the use of DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations it may be desired to prevent Content-Aware Rules from being applied to a specific group of client computers. To do so, return the previously defined Content-Aware Rules to the unconfigured state. All undefined DeviceLock Service settings are ignored by client computers.

### **To undefine Content-Aware Rules**

1. If using the DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Do one of the following:
  - In the case of rules for devices, expand the **Devices** node.
  - In the case of rules for protocols, expand the **Protocols** node.
3. Under the **Devices** node or **Protocols** node, right-click **Content-Aware Rules**, and then click **Undefine**.

## Deleting Content-Aware Rules

It is possible to delete individual Content-Aware Rules when they are no longer required.

### **To delete a Content-Aware Rule**

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.

- b. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using the DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Do one of the following:
    - In the case of a rule for devices, expand the **Devices** node.
    - In the case of a rule for protocols, expand the **Protocols** node.
  3. Under the **Devices** node or **Protocols** node, do one of the following:
    - Expand **Content-Aware Rules**, right-click the user or group to which the rule is applied, and then click **Delete user**.  
*When a user or group is deleted, the rule associated with this user or group is automatically deleted.*
    - OR -
    - Expand **Content-Aware Rules**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
    - OR -
    - Right-click **Content-Aware Rules**, and then click **Manage**. In the lower-left pane of the dialog box that appears, under **Users**, select the user or group to which the rule is applied. In the lower-right pane of that dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.  
*You can select multiple rules to delete by holding down the SHIFT key or the CTRL key while clicking them.*

# Digital Fingerprints

## Digital Fingerprinting Technique

Digital fingerprinting is a technique that DeviceLock employs to identify data transmitted across various devices and network protocols. This technique leverages the concept of mapping documents or files to collections of relatively short alphanumeric strings (hashes) referred to as digital fingerprints that can help to uniquely identify the data held in the document or file.

When using this technique, DeviceLock takes digital fingerprints from samples of sensitive documents and then compares them with the digital fingerprints of the documents being inspected. If the “fingerprints match” percentage exceeds the desired threshold as configured, the documents in question are then considered “sensitive” and subjected to the desired security action.

The use of digital fingerprints provides for identifying and protecting information held in files or transmitted over a network. For example, one can use them to identify financial data stored in MS Office documents, business information stored in PDF files, or source code stored in text files. Digital fingerprints can also be used to identify and protect non-text files (such as images, design drawings, and multimedia files), as well as to identify binary content attempting to be copied from one file to another.

Digital fingerprints can be used to identify full copies as well as pieces of documents, even if the document has been changed. They allow the contents of the document to be identified reliably, despite its possible distortion caused by adding non-essential information (individual characters, insignificant words, etc.).

Digital fingerprints are especially efficient when identifying standard documents that change insignificantly. For example, they make it easy to identify filled contracts that differ only in the second parties’ data. By reliably identifying data held in documents and files, digital fingerprints help track and protect sensitive information, thus providing for the scalable application of protective controls to that information as it flows across the corporate network and/or to peripheral user devices.

## How It Works

The digital fingerprinting technique is based upon the interaction of the following elements:

- [Content-aware rules](#)
- [Content groups](#)
- [Classifications of digital fingerprints](#)
- [Digital fingerprints of documents and files](#)
- [Digital fingerprints database](#)
- [Match percentage](#)
- [Normalization of fingerprints](#)

### **Content-aware rules**

Content-aware rules can leverage logical “content groups” of the Digital Fingerprints filter type for data analysis based on digital fingerprints. Such rules can be applied to both devices and network protocols, thus enabling the use of digital fingerprints to control content access/sending permissions, content-aware shadowing, and/or simple content detection.

### ***Content groups***

Content groups of the Digital Fingerprints filter type implement content inspection using digital fingerprints. Each group of this type references a certain classification of digital fingerprints, and would allow for the specification of a minimum percentage of fingerprint matching (referred to as threshold) that is required for assigning that classification to the content being inspected.

### ***Classifications of digital fingerprints***

Confidential documents and other information assets requiring protection can be classified according to classifications with certain levels of importance or secrecy (e.g. “Restricted”, “Confidential”, “Secret”, and “Top Secret”). Their digital fingerprints are classified to the respective classifications as well, so that the classification of each level holds digital fingerprints of information classified with the corresponding importance level. Each classification can be considered as a container that holds digital fingerprints of information samples classified to a certain level of importance or secrecy. Classifications are ordered according to that level.

DeviceLock provides a number of built-in classifications, and allows the addition of more custom ones. Their order by importance level can be changed when needed; however, the level of the built-in classification “Unclassified” is always lower than the level of any other classification and it cannot be raised. The “Unclassified” digital fingerprints have the lowest possible level regardless of whether or not they are encountered in other classifications.

### ***Digital fingerprints of documents and files***

A collection of hashes that uniquely identify a document or file and its contents is referred to as the digital fingerprint of that document or file. Fingerprints of sample documents and files of known classification can be stored in the database, where they are assigned that same classification. Then, the documents and files being inspected can be classified by comparing their fingerprints with those from the database. Thus, the collection and storage of fingerprints over time has a key role in the classification of documents and files going forward.

### ***Digital fingerprints database***

The DeviceLock Enterprise Server stores digital fingerprints of information samples provided to it (such as documents and files) in the fingerprints database, and allows for the management of fingerprints held in that database. Fingerprints are grouped by classification of their source. For example, fingerprints of “Secret” document samples are included in the “Secret” classification.

The database is serviced by tasks running on the server. For each classification, tasks can be created that process certain information sources (such as sets of documents) deliberately selected to the given classification. For example, a task for the “Secret” classification may be configured to process a folder with samples of “Secret” files. The fingerprints created by this task belong to the “Secret”



classification, and they can be used to identify other documents or files as “Secret” by matching the fingerprints of those documents or files with the fingerprints of the samples of “Secret” files.

### ***Match percentage***

When inspecting an information source (such as a document or file), DeviceLock can compare the source’s fingerprints with those of a certain classification in the database, and calculate their match percentage. If the match percentage exceeds the configured threshold, DeviceLock classifies the inspected information accordingly. For “Top Secret” documents, the match threshold might be relatively low as even small pieces of such documents may contain very important information. Conversely, for a document to be recognized as “Unclassified”, a large amount of its fragments must match with samples of “Unclassified” documents, so the match threshold must be relatively high. The match threshold value is selected when configuring a fingerprints content group for content-aware rules.

The match percentage is calculated as the greater of two values:

- The percentage of the source’s fingerprint elements that match the database-stored fingerprints of the given classification
- The total percentage of the elements of the database-stored fingerprints of the given classification that match the source’s fingerprints

The first value responds to a situation where the source contains fragments of various samples of sensitive information; the second value enables the correct classification of the source when it contains samples of sensitive information along with a large amount of non-sensitive information. Together these two values allow for proper handling of most cases of digital fingerprint-based identification of content.

### ***Normalization of fingerprints***

To optimize and expedite the process of matching, the fingerprints in the database are exposed to normalization: the elements of the “Unclassified” fingerprints are removed from all fingerprints held in other classifications. This assumes that “Unclassified” documents certainly do not contain sensitive information. If a document got in the classification “Unclassified”, the information held therein will not be identified as “Secret” or “Confidential”, even if its fingerprints are available in other classifications.

## **Fingerprints Collection and Storage**

Samples of information assets (documents, files, etc.) that have their fingerprints collected and stored in the database are referred to as fingerprint sources. Samples may be modified, added, or removed, or their secrecy level may change with time. For the database to accommodate all those changes, the server runs classification tasks on a regular basis, which will update the fingerprints storage as described below.

Information samples are processed and their fingerprints are created by tasks on the DeviceLock Enterprise Server. Each task attributes to a certain classification, and assigns it to the fingerprints

that it creates. For instance, fingerprints created by a task of “Confidential” classification are attributed to that same “Confidential” classification.

On every run, the task may inspect files in a particular folder. For each file, the task first creates the fingerprints of the file and compares them with the fingerprints from the database. The further processing of the file’s fingerprints depends upon comparison results such as:

- The classification already holds a fingerprint whose source has the same check sum, path, and name as the file being inspected. In this case, the task does not make changes to the fingerprints storage. However, in the case of a different path or name, the file is specified as one more source of that fingerprint in the database.
- The file’s check sum differs from the source’s check sum of an existing fingerprint, but the file’s fingerprint matches the existing fingerprint to some extent. In this case, the result of the task depends upon the percentage of matching elements of those fingerprints.  
If the percentage of matching elements does not exceed the configured threshold, the file’s fingerprint is added to the database as a new fingerprint, with that file specified as its source.  
If the percentage of matching elements exceeds the configured threshold, then the file’s fingerprint is specified as a new version of the existing one in the database. In this case, the file is specified as one more source of that fingerprint if its path or name differs from the path and/or name of other sources.
- The file’s fingerprint does not match any one fingerprint from the database. In this case, the file’s fingerprint is added to the database as a new fingerprint, with that file specified as its source.

Even if the source of a fingerprint is removed, the fingerprint remains in the database. DeviceLock administrators can delete fingerprints or their individual versions by hand using the DeviceLock Management Console.

## About Versioning Threshold

The versioning threshold determines whether to create a new fingerprint or merely add a new version to an existing fingerprint. The DeviceLock Enterprise Server specifies separate thresholds for text content (such as text files) and for binary content (such as image files).

Many files hold content of both types. For instance, Microsoft Word documents are binary files that can contain text and images. Fingerprints of files with mixed contents hold elements identifying text content and elements identifying binary content. When classifying such a “mixed” fingerprint, the server applies both thresholds, and separately assesses the match percentages for “text” and “binary” elements of the fingerprint. This results in the following effects:

- The fingerprint of a text file can be classified as a fingerprint version for a file with mixed contents, and vice versa, a “mixed” fingerprint can become a fingerprint version for a text file.
- The fingerprint of a binary file containing no text can be classified as a fingerprint version for a file with mixed contents, and vice versa, a “mixed” fingerprint can become a fingerprint version for a binary file with no text contents.

## Fingerprints Matching

To check information, such as files, documents, or messages, by matching with the fingerprints database, DeviceLock uses content-aware rules based on Digital Fingerprints content groups. The group determines the classification of the fingerprints to be applied, and specifies whether to require an exact match or a partial match. In case of partial match, the group defines the match threshold in percentage terms.

As the fingerprints database is hosted on DeviceLock Enterprise Server while content-aware rules are processed locally on client computers, DeviceLock Service requests the server to evaluate the fingerprints of the information being inspected. For this reason, at least one server instance must be specified in the DeviceLock Service settings. To improve fault tolerance and/or performance in larger sites, there can be specified two or more operational server instances.

## What If Server's Fingerprints Database Is Unavailable to Client?

If a DeviceLock Enterprise Server or its fingerprints database is unavailable, the local client's DeviceLock Service cannot apply fingerprint-based rules or "Complex" rules that contain Digital Fingerprints rule options. In this case, DeviceLock Service blocks attempts to transfer information that must be inspected by those rules by default. For example, if a rule controls the transferring of sensitive information by checking its fingerprints, but the fingerprints database server is unavailable, DeviceLock Service will not allow transferring information that must be checked by that rule.

## Inspecting fingerprints within archives

Suppose DeviceLock Service has the [Archives content inspection on read](#) and/or [Archives content inspection on write](#) parameter enabled. In this case, when applying content-aware rules to archive files, DeviceLock Service applies them to each file found in the archive (see the [Inspection of files within archives](#) feature description). However, it may skip inspecting fingerprints of files within an archive if it has detected an exact match of the archive file with a source file of a certain fingerprint from the database.

Consider the following scenario:

- DeviceLock Service has the [Archives content inspection on read](#) and/or [Archives content inspection on write](#) parameter enabled.
- A Digital Fingerprints content group has the **Exact file match** option enabled (see [Dialog box for configuring a Digital Fingerprints group](#)).
- A rule uses that group to inspect an archive file, and detects that the check sum of the archive file matches the check sum of a certain fingerprint source file found in the database.

In this scenario, DeviceLock Service applies the rule to the archive file without inspecting fingerprints of files within the archive. The entire archive would be allowed or denied in accordance with the rule settings.

However, if the check sum of the archive file does not match the check sum of any fingerprint source file, then DeviceLock Service would apply the rule to each file within the archive. In case of an “allow” rule, the archive is allowed if the rule allows each file within the archive; in case of a “deny” rule, the entire archive is denied if the rule denies at least one file within the archive.

## Getting Started Using Digital Fingerprints

To use digital fingerprints, a DeviceLock administrator would collect samples of documents and files that the organization wants to protect, and classify them on the DeviceLock Enterprise Server by using classification tasks that take fingerprints of each sample file and its contents. For details, see [Fingerprinting Tasks](#). The files to fingerprint can be stored in the server’s local folder or in a shared network folder. Copying files to the computer running DeviceLock Enterprise Server is not required; however, the server must have sufficient rights to access and read those files in their location.

Then, a DeviceLock administrator would create content groups referencing classifications of fingerprints and configure content-aware rules based on those content groups. For details, see [Digital Fingerprints Content Groups](#). As the fingerprints database is hosted on the server while content-aware rules are processed on client computers, at least one DeviceLock Enterprise Server must be specified in the DeviceLock Service policy settings. For details, see [Service Options for Digital Fingerprints](#). The DeviceLock Service can then employ the rules to check submitted information by matching its fingerprints with the fingerprints stored in the database.

To take an example, suppose the samples of confidential documents and files are several MS Office Word, Excel, and PowerPoint documents, and a number of image files (such as PNG or JPEG). The DeviceLock administrator first creates and runs a task of classification “Confidential” that points to the folder containing those documents and image files. As a result, their fingerprints will have been created and stored in the database of the DeviceLock Enterprise Server. The administrator then creates a Digital Fingerprints content group with the classification level of “Confidential”. When creating the group, it is possible to set the match threshold, i.e. a minimum percentage of fingerprint matching that is required for assigning the given classification level to the content being inspected. Suppose the threshold is set to 50%. Finally, the administrator sets up a content-aware rule based on the Digital Fingerprints group that was created. This rule can be configured, for example, to control access, shadow copying, and/or detection of content.

When applying this rule to a file, the DeviceLock Service checks the file, and the file’s text-based content if it can be extracted, by matching their fingerprints against the fingerprints from the “Confidential” classification held in the database. If the fingerprint match percentage is 50% or more in this example, the rule takes effect and causes the DeviceLock Service to act as specified in the ContentLock or Discovery rule settings (block, allow, shadow, alert, detect, apply remedy, etc.).

## Administering Digital Fingerprints

The DeviceLock Enterprise Server keeps digital fingerprints of information samples (such as documents and files) provided to it, and allows for the management of fingerprints creation, classification, and storage:

- [Fingerprinting Options](#) - View or change fingerprint management settings, such as the fingerprint version threshold.
- [Fingerprinting Tasks](#) - Configure, run, or inspect tasks that take and classify fingerprints of information samples. Create and configure additional classifications, if needed.
- [Fingerprints Database](#) - View information about stored fingerprints, their versions, and their sources. If needed, add or remove fingerprints, or remove their individual versions.
- [Fingerprints Log Viewer](#) - Review events related to the management and processing of fingerprints in the DeviceLock Enterprise Server.

## Fingerprinting Options

The fingerprint versioning threshold is among the fingerprinting options. It determines the conditions under which the server creates new fingerprints instead of adding new versions to fingerprints that already exist in the database (see [Fingerprints Collection and Storage](#) for details).

To view these options in the details pane, select **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprinting Options** in the console tree.

The following options are available:

- [Versioning threshold for text](#) - Determines whether to consider a given fingerprint of a sample of text content to be a new fingerprint or a version of an existing one.
- [Versioning threshold for binary](#) - Determines whether to consider a given fingerprint of a sample of binary content to be a new fingerprint or a version of an existing one.

When classifying fingerprints of mixed content (such as Microsoft Word documents), the server applies both thresholds, and separately assesses the match percentages for “text” and “binary” elements of the fingerprint. For details, see [About Versioning Threshold](#).

### Versioning threshold for text

This option applies to text content (such as text documents), and determines the minimum percentage of matching fingerprint elements that allows the fingerprint of the given content to be considered as a version of an existing fingerprint. If the percentage of matching elements is lower than this threshold, the server adds the new fingerprint to the database; otherwise, it adds a new version to the existing fingerprint.

To specify the desired percentage value, double-click this option in the details pane and use the dialog box that appears.

See also:

[Fingerprints Collection and Storage](#)

### Versioning threshold for binary

This option applies to binary content (such as image files), and determines the minimum percentage of matching fingerprint elements that allows the fingerprint of the given content to be considered as

a version of an existing fingerprint. If the percentage of matching elements is lower than this threshold, the server adds the new fingerprint to the database; otherwise, it adds a new version to the existing fingerprint.

To specify the desired percentage value, double-click this option in the details pane and use the dialog box that appears.

See also:

[Fingerprints Collection and Storage](#)

## Fingerprinting Tasks

Samples of information assets that require protection (documents, files, etc.) are processed, and their fingerprints are created and stored, by tasks on the server. Each task attributes to a certain classification, and assigns it to the fingerprints that it creates. For instance, fingerprints created by a task of “Confidential” classification are attributed to that same “Confidential” classification.

The classifications are listed in the console tree under **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprinting Tasks**. To view the tasks of a certain classification, select that classification in the console tree, under **Fingerprinting Tasks**.

The shortcut menu on the **Fingerprinting Tasks** node provides the following command:

- **Edit Classifications** - Use this command to create, rename, or delete custom classifications. You can also raise or lower the level of a custom classification. See [Managing Classifications](#) for details.

When **Fingerprinting Tasks** is selected in the console tree, the details pane lists the names of the classifications that are currently available on the server. The shortcut menu on each classification provides the following commands:

- **Create Task** - Create and configure a new task for the selected classification (see [Creating Tasks](#)).
  - **Refresh** - Update the list in the details pane with the latest information.
- These commands are also available on each classification under **Fingerprinting Tasks** in the console tree (see [Managing Existing Tasks](#)).

Task management involves the following activities:

- [Creating Tasks](#)
- [Managing Existing Tasks](#)
- [Viewing Task Run Reports](#)

## Creating Tasks

Creating a task requires the following steps:

1. Choose the classification for which to create the task.

Each task attributes to a certain classification, and assigns it to the fingerprints that it creates. For instance, fingerprints created by a task of “Confidential” classification are attributed to that same “Confidential” classification.

2. Execute the **Create Task** command for the desired classification under **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprinting Tasks**.

Select this command from the shortcut menu of the desired classification in the console tree or details pane, or from the shortcut menu of a task that already exists in that classification.

3. Configure the task settings in the dialog box that appears (see [Dialog box for configuring a task](#)).

## Dialog box for configuring a task

In the dialog box for configuring a task, the administrator can view or change the following settings:

- **Task name** - The name that serves to identify the task.
- **Classification level** - The classification of the fingerprints being created by the task. This setting is assigned the classification that was selected when creating the task.
- **Active** - Select this check box to enable the server to the task automatically. When this check box is cleared, the task can only be run by hand using the console.
- **Schedule** - The following settings specify when the server should be running the task:
  - **Update automatically when directory contents change** - The server runs the task whenever it detects changes in any of the folders that are subject to processing by that task.

---

### Note

The server may delay the running of the task for about half a minute after detecting changes.

---

- **Update every <number> minutes** - The server runs the task every time upon the lapse of the specified number of minutes. You can set the desired number of minutes.

If the **Active** check box is cleared, the **Schedule** settings have no effect.

- **Options** - The following settings specify the documents and files to be processed by the given task:
  - **Look for** - The names of the files for processing. To separate names, use a semicolon (;). To denote any group of characters within a name, use an asterisk (\*). An empty field means it is looking for any files.  
Example: \*.doc; \*.docx matches any files with the doc or docx file name extension.
  - **Look in** - Path to the folder containing the files for processing. This can be a local folder or a network folder. The server must have sufficient access rights to read files in that folder. To specify a network folder, use its UNC path (\\server\share\folder). Multiple folders can be specified by separating their paths with a semicolon (;).
    - **Including subfolders** - When this check box is selected, the task will process files contained both in the folder specified in the **Look in** box and in all its subfolders. Otherwise, the task processes only the files contained directly in the folder specified, disregarding subfolders.

- **Unpack archives** - When this check box is selected, the task will process files contained in archive files, such as in .zip files. Otherwise, the task handles archive files the same way as any other binary files.
- **Modified** - When this check box is selected, the task processes only the files that match a certain condition imposed on the last modification date/time of the file. The following conditions are available:
  - **Before than** - The last modification date/time must be earlier than the specified date/time.
  - **After than** - The last modification date/time must be later than the specified date/time.
  - **Between** - The last modification date/time must fall within the specified date/time range.
  - **Not older** - After the last modification date/time, must lapse no more than the specified number of seconds, minutes, hours, days, weeks, months, or years.
  - **Older than** - After the last modification date/time, must lapse more than the specified number of seconds, minutes, hours, days, weeks, months, or years.
- **File size** - When this check box is selected, the task processes only the files that match a certain condition imposed on the size of the file. The following conditions are available:
  - **Equal to** - The size must be equal to the value specified.
  - **Less than** - The size must be less than the value specified.
  - **More than** - The size must be more than the value specified.
  - **Between** - The size must be between two values specified.
- **Attributes** - When this check box is selected, the task processes only the files with the specified attributes. You can specify NTFS file system attributes such as **System**, **Hidden** and/or **Encrypted**.

## Managing Existing Tasks

To view the tasks of a certain classification, select that classification in the console tree, under **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprinting Tasks**. The details pane provides the following information on each task:

- **Task name** - The name that identifies the task.
- **Status** - One of the following values:
  - **Running (X of Y files processed)** - Task execution is in progress. The number of files processed by the task at this time (X) and the total number of files to be processed (Y) are indicated in parentheses.
  - **Waiting** - The task is enabled and waiting for the next scheduled or automatic run.
  - **Inactive** - The task is not enabled and it can be run only by hand.  
The task is enabled when it has the **Active** check box selected. If the task is enabled, its next run is determined by the **Schedule** setting. For more information, see [Dialog box for configuring a task](#).
- **Last update time** - The date and time that this task was last run.



- **Fingerprints added** - The number of fingerprints created by the task during the last run. The value in parentheses indicates the total number of fingerprints created by this task during all runs.
- **Fingerprints updated** - The number of fingerprints updated by the task during the last run. Updating fingerprints means adding new versions and/or new sources to the fingerprints that already exist in the database.
- **Schedule** - One of the following values:
  - **Update automatically** if the task has the **Update automatically when directory contents change** option selected.
  - The date and time of the next run if the task has the **Update every <number> minutes** option selected.

The upper part of the details pane displays a list of tasks. The lower part of the details pane contains reports on executing the task selected in that list. The reports provide a history of task execution, along with details on the fingerprint sources that have been processed during each run of the task. For more information, see [Viewing Task Run Reports](#).

The shortcut menu on a classification in the console tree provides the following commands:

- **Create Task** - Create and configure a new task for that classification (see [Creating Tasks](#)).
- **Refresh** - Update the task list of that classification with the latest information. This command does not update task execution reports. To update the execution reports for a particular task, use the **Refresh** command on that task in the details pane.

The shortcut menu on a task in the details pane provides the following commands:

- **Run now** - Start the selected task. You can use this command to run a task by hand, regardless of the task schedule.
- **Create Task** - Create and configure a new task for the same classification as the selected task (see [Creating Tasks](#)).
- **Edit Task** - View or change the settings of the selected task. This command opens a dialog box to view or change the task name, schedule, and other options (see [Dialog box for configuring a task](#)).
- **Delete Task** - Delete the selected task. Deleting a task does not delete the fingerprints created by that task. For information on how to review and, if needed, delete fingerprints from the database, refer to the section [Fingerprints Database](#).
- **Clear history** - Delete all execution reports of the selected task. The command prompts to confirm the deletion, and leaves in place of the deleted reports a message to inform about how many reports were deleted as well as by whom and from what computer the deletion was performed.
- **Refresh** - Update the execution reports of the selected task with the latest information. This command does not update the list of tasks in the details pane. To update the task list of a particular classification, use the **Refresh** command on that classification in the console tree.

## Viewing Task Run Reports

When a classification under **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprinting Tasks** is selected in the console tree, the upper part of the details pane displays a list of tasks that handle fingerprints for that classification. The lower part contains reports on executing the task selected in that list.

The lower part of the details pane lists the task runs in chronological order, with the last run displayed first in the list. Only those runs are listed that made any substantial changes to the database (such as adding fingerprints). Other non-eventful runs are not included in the list.

The list of task runs provides the following information about each run:

- The run report header composed of the following items:
  - <date-time started> - <date-time completed>  
These items indicate the date and time that the task was started and completed.
  - The way the task was started:
    - **Scheduled** - Run by a schedule. The task has the **Update every <number> minutes** option selected.
    - **Automatic** - Run caused by a change in folder contents. The task has the **Update automatically when directory contents change** option selected.
    - **Manual** - Run on command from the management console.
- A list of files that the task processed during the run, with the following information on each file:
  - **File name** - The name of the file.
  - **Classifications: %** - A list of classifications that hold fingerprints partially or fully matching the file's fingerprint. For each classification, the list displays the percentage of matching fingerprint elements of this file.
  - **Full path** - The full path to the file. If the file is contained in an archive file, the full path is composed of the full path to the archive file and the path to the file within the archive.

## Managing Classifications

Each classification can be considered as a container that holds digital fingerprints of information classified to a certain level of importance or secrecy. Classifications are ordered according to that level. When a given information sample matches fingerprints in several classifications, then it is considered to belong to the classification of the lowest level.

DeviceLock provides the following built-in classifications:

- Top Secret (highest level)
- Secret
- Confidential
- Restricted
- Unclassified (lowest level)

This order of built-in classifications cannot be changed; however, you can add custom classifications and change their order around built-in ones when needed. Note that any classification cannot be placed below the “Unclassified” classification level.

To add, view, or change custom classifications, use the **Edit Classifications** command from the menu of the **Fingerprinting Tasks** node. For example, select **DeviceLock Enterprise Server > Digital Fingerprints** in the console tree, right-click **Fingerprinting Tasks** in the details pane, and then click **Edit Classifications** on the shortcut menu.

The **Edit Classifications** command opens a dialog box where administrators can:

- View the ordered list of all classifications (both built-in and custom) available on the server.
- Create a custom classification. Click the **Add** button, and enter the name of the new classification.
- Change the level of the custom classification. Select a classification in the list, and then use the “Up” and “Down” buttons next to the **Rename** button.
- Change the name of the custom classification. Select a classification in the list, click the **Rename** button, and enter a new name.
- Delete a custom classification. Select the classification in the list, and click the **Delete** button.

---

#### **Important**

When a custom classification is deleted, the server automatically deletes all tasks and fingerprints related to that classification.

---

DeviceLock does not allow built-in classifications to be deleted, renamed or reordered. The built-in classification “Unclassified” always has the lowest level.

## Fingerprints Database

The DeviceLock Enterprise Server stores digital fingerprints of information samples provided to it (such as documents and files) in the fingerprints database, and allows for the management of fingerprints held in that database. Fingerprints are grouped by classification of their source. For example, fingerprints created by a task of the “Secret” classification are included in the “Secret” classification.

The fingerprint classifications that exist in the database are listed in the details pane when **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprints Database** is selected in the console tree. The list provides the following details on each classification:

- **Classification** - The name of the classification.
- **Quantity** - The number of fingerprints in the database that are attributed to this classification.
- **Size** - The total size of fingerprints in the database that are attributed to this classification.
- **Last updated time** - The date and time that fingerprints were last added or updated in this classification.
- **Last updated by** - The name of the task that last added or updated fingerprints in this classification. If the last change in this classification was the adding of fingerprints by hand, the account name of the user who added the fingerprints is displayed instead of a task name.

- **Frequency matching** - The counter showing how many times fingerprints from this classification triggered when inspecting content by fingerprint-based rules.  
This counter is incremented by one when a rule detects that the inspected content matches at least one fingerprint from this classification. When processing such a rule, the counter is only incremented by one even if the inspected content matches several fingerprints in this classification.
- **Classification effectiveness** - The percentage showing how many times fingerprints from this classification triggered, as compared to the total number of times the fingerprints from all classifications triggered.  
As a single fingerprint may possess elements attributed to different classifications, the sum of effectiveness values by all classifications may exceed 100%.

The shortcut menu on each classification provides the following commands:

- **Add fingerprint** - Select the information sample, such as a document or file, of which the fingerprint needs to be taken. The fingerprint of the selected sample will be added to the classification for which this command is performed (see [Adding Fingerprints Manually](#)).
- **Refresh** - Update the list in the details pane with the latest information.  
These commands are also available on each classification under **Fingerprints Database** in the console tree (see [Viewing Fingerprint List](#)).

Fingerprint-database management involves the following activities:

- [Viewing Fingerprint List](#)
- [Viewing Detailed Fingerprint Information](#)
- [Adding Fingerprints Manually](#)

## Viewing Fingerprint List

All fingerprint classifications that exist in the database are listed in the console tree under **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprints Database**. To view the fingerprints attributed to a certain classification, select that classification in the console tree, under **Fingerprints Database**.

The details pane lists the fingerprints, with the following details provided on each one:

- **Name** - The name that identifies the fingerprint. When adding the fingerprint of a file to the database, the server assigns it the name of that file.

---

### Note

A record in parentheses following the name of the fingerprint that was added by hand identifies who and from what computer added that fingerprint (see also [Adding Fingerprints Manually](#)).

---

- **Conformity (%)** - The percentage of fingerprint elements (hashes) that conform to the selected classification.  
Some elements of a fingerprint may be part of other fingerprints that belong to lower-level classifications. For example, a fingerprint placed into the "Secret" classification can be sourced

from a document where just a part of which serves as a source of another fingerprint belonging to the classification "Unclassified". In this case, some elements of the "Secret" fingerprint will be attributed to the classification "Unclassified". Since elements attributed to a lower-level classification are not considered to conform to a higher-level classification, the **Conformity** value could be less than 100%.

---

**Note**

When calculating the **Conformity** value, the hashes of all versions of the fingerprint are evaluated. As a result, this value for a particular version of the fingerprint (for example, for its latest version) may be higher than for the entire fingerprint.

---

- **Date added** - The date and time that the fingerprint is initially created.
- **Date updated** - The date and time that the fingerprint is last updated.  
Updating a fingerprint occurs every time a new version and/or a new source of the fingerprint is added.
- **Versions** - The number of versions of this fingerprint that exist in the database.
- **Sources** - The total number of registered sources of this fingerprint, with the number of "active" sources indicated in parentheses. A source is considered active if it exists (has not been deleted, moved or renamed) and is scanned by some fingerprinting task on a regular basis.
- **Source type** - The type of the fingerprint source:
  - **Text** - The source holds solely text content (for example, this is a text file). The fingerprint is taken from the source's text content.
  - **Binary** - The source holds no text content (for example, this is an image file). The fingerprint is taken from the source's binary data.
  - **Text/Binary** - The source holds both text and binary content (for example, this is a Microsoft Word document or .pdf file). The fingerprint is taken from each content type separately.
- **Size** - The size of this fingerprint in the database.
- **Frequency matching** - The counter showing how many times this fingerprint triggered when inspecting content using fingerprint-based rules.  
This counter is incremented by one in any of the following occurrences:
  - A rule with the **Exact file match** parameter enabled detects that the check sum of the inspected content matches the check sum of the given fingerprint's source file.

---

**Note**

The rule may not trigger if its classification has no elements of the given fingerprint (the fingerprint has the **Conformity** value of zero in this classification). Nonetheless, if the check sums match, the counter is incremented by one for the classification containing that fingerprint.

---

- A rule with the **Threshold** setting specified (the **Exact file match** parameter is disabled) detects any of the following cases:
  - The match percentage of the given fingerprint with the inspected content exceeds the value of the **Versioning threshold for text** or **Versioning threshold for binary** parameter (see

[Fingerprinting Options](#)).

- This fingerprint to the most extent matches the inspected content by the number of matching elements (hashes) in comparison with other fingerprints available in the database.

In either case, the counter is incremented by one regardless of whether the content inspection rule has triggered.

---

**Note**

In any of the occurrences listed above, the counter is incremented within all classifications to which the fingerprint conforms.

---

- **Effectiveness** - The percentage showing how many times this fingerprint triggered when inspecting content using fingerprint-based rules, as compared to the total number of times the fingerprints from this classification triggered.

The shortcut menu on a classification in the console tree provides the following commands:

- **Add fingerprint** - Select the information sample, such as a document or file, of which the fingerprint needs to be taken. The fingerprint of the selected sample will be added to the classification for which this command is performed (see [Adding Fingerprints Manually](#)).
- **Refresh** - Update the fingerprint list of the selected classification with the latest data. This command does not update detailed information shown under the fingerprint list. To update the information about a particular fingerprint, use the **Refresh** command on that fingerprint in the details pane.

The shortcut menu on a fingerprint in the details pane provides the following commands:

- **Add fingerprint** - Same as on the classification in the console tree.
- **Remove fingerprint** - Delete the fingerprint on which this command is performed. The **Remove fingerprints** command that appears in case of a selection of two or more fingerprints provides the ability to delete all the selected fingerprints at a time.
- **Refresh** - Update the detailed information about the selected fingerprint with the latest data (see [Viewing Detailed Fingerprint Information](#)). This command does not update the list of fingerprints in the details pane. To update the fingerprint list of a particular classification, use the **Refresh** command on that classification in the console tree.

## Viewing Detailed Fingerprint Information

When a classification is selected under **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprints Database** in the console tree, the upper part of the details pane lists the fingerprints attributed to that classification. In the lower part, the console displays information about versions and sources of the fingerprint selected in that list.

Fingerprints held in the database are taken from certain information samples (such as documents or image files), referred to as fingerprint sources. The server registers these sources with the database when adding or updating fingerprints.

When initially adding a fingerprint, the server registers its source as the only source of that fingerprint. For fingerprints existing in the database, the server may register additional sources. Thus, the server registers a new source file for an existing fingerprint in the following cases:

- The task has detected that the path or name of the earlier-registered source file changed. The file registers as a new source with the respective path and name.
- The task has added the fingerprint of a certain file as a version of the existing fingerprint and the file is not among the registered sources of that fingerprint. The file registers as a new source along with the new version of the fingerprint.

Having created a fingerprint, the server may add it to the database as a new fingerprint or as a version of another fingerprint that already exists in the database. A version is added if the percentage of matching elements of the existing fingerprint and the newly created one exceeds the threshold value specified by the respective setting (see [Fingerprinting Options](#)).

Different versions of a fingerprint can be created by tasks of different classifications. As a result, the elements of the fingerprint are distributed among multiple classifications. Such a fingerprint is said to conform to multiple classifications, with some (non-zero) percentage of conformity to each classification.

---

**Note**

When matching the inspected content to a fingerprint from the database, a comparison is performed with the elements (hashes) of all versions of that fingerprint.

---

The console provides the following information about the versions and sources of each fingerprint:

- **Version** - The number of the version. Initially the fingerprint has a single version with the number of one (1). Adding every new version increments the version number by one.  
If necessary, the administrator can delete individual versions of the fingerprint by clicking the red X in the **Remove** column next to a version number in the list.
- **Path** - The full path and name of the fingerprint's source. This may be a path on a local disk, or a UNC path on a network file server. If the source is contained in an archive file, the full path is composed of the path to the archive file and the path to the source within the archive. Some versions may contain fingerprint elements (hashes) of multiple sources. In this case, the path and name of all those sources are listed in the **Path** column next to the number of the version.

The color of the icon in the **Path** column indicates the state of the fingerprint source:

- Green - Means that the source with the specified path and name exists and is scanned by some fingerprinting task on a regular basis.
- Gray - Appears in the following occurrences:
  - The fingerprint of the source was taken by hand (see [Adding Fingerprints Manually](#)).
  - The source with the specified path and name no longer exists (for instance, the source file has been renamed, moved or deleted).
  - The source is no longer scanned by fingerprinting tasks because of changes to task settings (these settings are described in [Dialog box for configuring a task](#)).

- **Date added** - The date and time that the server last added to the database the fingerprints of the source specified.
- **Last scan time** - The date and time when fingerprinting tasks last scanned the given source.
- **<Classification name> (%)** - The percentage of the fingerprint's elements (hashes) that conform to the classification specified. The list may contain several names since different elements of the fingerprint may conform to different classifications.

## Adding Fingerprints Manually

Normally, the fingerprints database is populated by using tasks (see [Fingerprinting Tasks](#)). It is also possible to add fingerprints directly, without having to create, configure and run a task. This feature is intended for the prompt fingerprinting of files to the database.

To promptly fingerprint files to the database, use the **Add fingerprint** command available on each classification in the [Fingerprints Database](#) node. Fingerprints are added to the classification for which this command is performed. The command prompts to select files and then takes their fingerprints and saves them in the database.

The **Add fingerprint** command uses a standard dialog box for selecting files, supplemented with the following option that is in effect when an archive file (such as a .zip file) is selected:

- **Unpack archives** - If this check box is selected, the command takes the fingerprint of each file found in the archive. Otherwise, the command handles the archive file the same way as any other binary file, and only takes the fingerprint of that file.

Upon completion of the command, a dialog box appears that lists the added fingerprints with the following details on each one:

- **Name** - The name that identifies the fingerprint. When adding a fingerprint to the database, the server assigns it the name of the file of which the fingerprint was taken.
- **Source type** - The type of the file to fingerprint or dash in case of empty file. Possible types:
  - **Text** - The file holds solely text content (for example, this is a text file). The fingerprint is taken from the text content.
  - **Binary** - The file holds no text content (for example, this is an image file). The fingerprint is taken from the binary data.
  - **Text/Binary** - The file holds both text and binary content (for example, this is a Microsoft Word document or .pdf file). The fingerprint is taken from each content type separately.
- **<Classification name>** - The percentage of the fingerprint's elements (hashes) that conform to the classification specified. The list may contain several names since different fingerprints and their individual elements may conform to different classifications.
- **Full path** - The path and name of the file the fingerprint was taken from. This may be a path on a local disk, or a UNC path on a network file server. If the file is contained in an archive, displayed are the path to the archive and the path to the file inside the archive.
- **Information** - Operation outcome:



- **Added** - The fingerprint successfully taken and saved in the database.
- **Added, Corrupted data** - Unable to take the fingerprint of text content possibly due to text data corruption. The fingerprint has only been taken from the binary data.
- **Added, Password protected** - Unable to take the fingerprint of text content due to password protection of the text data. The fingerprint has only been taken from the binary data.
- **Already exists** - The fingerprint of the given file is already in the database.
- **Empty** - The file to fingerprint contains no data. The fingerprint is not created.
- **Error:** <message> - The error message if the fingerprint creation failed.

## Fingerprints Log Viewer

The Fingerprints Log holds records that help monitor events related to the management and processing of fingerprints in the DeviceLock Enterprise Server. Events caused by the following actions are logged:

- Changing fingerprints-related server settings, such as versioning thresholds (see [Fingerprinting Options](#)) or custom classifications (see [Managing Classifications](#)).
- Administering fingerprints-creation tasks (see [Fingerprinting Tasks](#)), such as starting, completing, adding, changing or deleting tasks, or deleting task execution reports.
- Adding fingerprints by tasks (see [Fingerprinting Tasks](#)) or by hand (see [Adding Fingerprints Manually](#)).
- Deleting fingerprints and/or their versions (see [Viewing Fingerprint List](#), [Viewing Detailed Fingerprint Information](#)).
- Processing fingerprints-related client requests, such as checking fingerprints upon request from DeviceLock Service or Discovery Agent (see [Applying Digital Fingerprints](#)). The log provides information about processing start and completion, and about errors if any occurred during request processing.

The information held in this log helps track changes to fingerprint management options and tasks, and facilitates the troubleshooting of issues related to fingerprint management and application.

To view the log, select **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprints Log Viewer** in the console tree. The details pane lists the events from the Fingerprints Log, with the following information provided for each event:

- **Type** - The event type can be one of the following:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Date/Time** - The date and time that the event occurred.
- **Event** - ID number of the event.
- **Task Name** - Indicates the fingerprinting task that caused the event or was affected by the event.
- **Classification Name** - Indicates the fingerprints classification relating to or affected by the event.








- **Information** - A description of the event that provides details on the actions performed and errors encountered.
- **Server** - The name of the computer running DeviceLock Enterprise Server that logged this event.
- **Record N** - Sequence number of the event record in the list.
- **Consolidation Server** - The name of the remote server from which this event was last received during log consolidation (see [Consolidating Logs](#)).
- **Consolidated Date/Time** - The date and time that this event was last received from the remote server during log consolidation (see [Consolidating Logs](#)).

## Managing the Fingerprints Log

The log can be managed by using commands from the shortcut menu:



- In the DeviceLock Management Console tree, expand **DeviceLock Enterprise Server > Digital Fingerprints**, and then right-click **Fingerprints Log Viewer** under the **Digital Fingerprints** node.  
- OR -
- In the DeviceLock Management Console tree, select **DeviceLock Enterprise Server > Digital Fingerprints > Fingerprints Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings**  - View or change the settings that limit the maximum number of event records the log may contain.
- **Save** - Save the log to the file you specify.
- **Refresh**  - Update the list of events with the latest information.
- **Filter**  - Display only the events that match the conditions specified.
- **Quick filters** - Choose from the following options to view the events that occurred during:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Clear**  - Delete all event records that currently exist in the log. This command also adds to the log a deletion record indicating how many records have been deleted as well as who performed the deletion and from what computer.

### *To view or change log settings*

1. Click **Settings** on the shortcut menu.
2. Use the options in the dialog box that appears (see [Fingerprints Log Settings](#)).

### ***To configure a log filter***

1. Click **Filter** on the shortcut menu.
2. Use the options in the dialog box that appears (see [Fingerprints Log Filter](#)).

## **Fingerprints Log Settings**

The dialog box for managing log settings is used to view or change the following parameters:

- **Control log size** - Select this check box to control the number of records in the log and delete outdated records. If this check box is cleared, all available disk space is used to store the log.
- **Keep events for last <number> days** - When this option is selected, the log stores records no older than the number of days specified (365 days by default).
- **Maximum log size: <number> records** - When this option is selected, the log stores no more than the specified number of records. With this option, you must choose the action to perform when the log reaches its maximum size:
  - **Overwrite events as needed** - New event records continue to be stored when the maximum log size is reached. Each record of a new event replaces the oldest record in the log.
  - **Overwrite events older than <number> days** - New event records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.
  - **Do not overwrite events (clear log manually)** - New event records are not added when the maximum log size is reached. To enable the server to add new records, old ones must be deleted by hand.

---

### **Note**

The server removes old records either by the date indicated in the **Date/Time** column (for records logged by the local server) or by the date indicated in the **Consolidated Date/Time** column (for records received from other servers using [consolidation](#)).

---

---

### **Important**

If the log has no space for new records and log settings do not allow the deletion of old records, then the server does not add any new records to the log.

---

To use default settings, click **Restore Defaults**. The default settings are as follows:

- Maximum log size: 10,000 records
- Overwrite events older than 7 days

## **Fingerprints Log Filter**

A filter causes the console to display only the event records that match the conditions specified in the dialog box for configuring the fingerprints log filter.

Two types of filter are available:

- **Include** - Display only the event records that match the condition specified. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab and specify conditions on that tab.
- **Exclude** - Do not display the event records that match the conditions specified. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab and specify conditions on that tab.

The filter can be temporarily disabled by clearing the **Enable filter** check box.

---

#### Note

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

When the filter is enabled, its conditions are defined by entering values in the following fields:

- **Event types** - Select check boxes to filter events by type:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- String fields intended to include or exclude event records depending upon whether event data matches the filter string specified. For example, to filter records by the name of the task that caused the event, specify a filter string in the **Task name** field. To filter records with certain event IDs, enter ID numbers separated by a semicolon in the **Event ID** field.

The following string fields are available:

- **Classification name** - The name of the fingerprints classification relating to or affected by the event.
- **Task name** - The name of the fingerprinting task that caused the event or was affected by the event.
- **Information** - A description of the event that provides details on the actions performed and errors encountered.
- **Server** - The name of the computer running DeviceLock Enterprise Server that logged the event.
- **Event ID** - The ID number of the event.

---

#### Note

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

- **From, To** - The time range settings to filter events by time they were logged by the server.
- **Consolidation** - The fields to filter by log consolidation-related data (see [Consolidating Logs](#)):
  - **Server** - The name of the remote server from which the event was last received during log consolidation. This field is case-insensitive, and allows the use of wildcards (\* and ?). To enter

multiple values, separate them with a semicolon (;).

- **From, To** - The time range settings to filter events by time they were last received from the remote server during log consolidation.

For each time range, the following settings are available:

- **From** - The beginning of the time range. Possible values:
  - **First Record** - Filter starting with the earliest date and time in the respective log field.
  - **Records On** - Filter starting with a particular date and time.
- **To** - The end of the time range. Possible values:
  - **Last Record** - Filter ending with the latest date and time in the respective log field.
  - **Records On** - Filter ending with a particular date and time.

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

## Applying Digital Fingerprints

To use digital fingerprints, the administrator collects samples of documents and files that the organization wants to protect, and classifies them on the DeviceLock Enterprise Server by using classification tasks that take fingerprints (see [Administering Digital Fingerprints](#)).

Configuring DeviceLock Service to apply fingerprint-based rules assumes the following activities:

- Indicate one or more DeviceLock Enterprise Servers that host the fingerprints database. For instructions, see [Service Options for Digital Fingerprints](#).
- Create and configure fingerprint-based content groups. For instructions, see [Digital Fingerprints Content Groups](#).
- Using those groups, set up content inspection rules as described earlier in this document, in the section [Content-Aware Rules \(Regular Profile\)](#).

## Service Options for Digital Fingerprints

To employ the digital fingerprinting technique, interaction is required between DeviceLock Services and at least one DeviceLock Enterprise Server. This is because the fingerprints database is on the

server whereas rules for checking fingerprints are applied on client computers (see [Fingerprints Matching](#) for details).

There are service options that govern what server to be used to check fingerprints. To view these options in the details pane, select **DeviceLock Service** > **Service Options** > **Digital Fingerprints** in the console tree.

The following options are available:

- [Use global DeviceLock Enterprise Server\(s\) settings](#) - Check fingerprints using the same server(s) specified for other operations (such as collecting audit and shadow logs or policy management).

---

**Important**

Only the server(s) specified for the “Everyone” account will be used.

---

- [DeviceLock Enterprise Server\(s\)](#) - Use dedicated servers to check fingerprints.

In case of certificate-based authentication, where a certain DeviceLock certificate’s public key is installed for DeviceLock Service, the private key of that certificate must be installed on the server that is intended to check fingerprints (for instructions, see [Server administrators and certificate](#)). Otherwise, fingerprint-based rules have no effect (for more information, see [What If Server’s Fingerprints Database Is Unavailable to Client?](#)).

## Use global DeviceLock Enterprise Server(s) settings

To enable or disable this setting, double-click it in the details pane.

When this setting is enabled, DeviceLock Service checks fingerprints using the server(s) specified for the “Everyone” account in the **Service Options** > [DeviceLock Enterprise Server\(s\)](#) setting.

When this setting is disabled, DeviceLock Service checks fingerprints using the server(s) specified in the **Service Options** > **Digital Fingerprints** > [DeviceLock Enterprise Server\(s\)](#) setting.

## DeviceLock Enterprise Server(s)

To enable this setting for checking fingerprints on dedicated DeviceLock Enterprise Server(s), disable the setting [Use global DeviceLock Enterprise Server\(s\) settings](#). Otherwise, the **DeviceLock Enterprise Server(s)** setting is unavailable.

When this setting is enabled, DeviceLock Service checks fingerprints by using the servers listed in this setting. Double-click the setting in the details pane; then, use the dialog box that appears to view or change the list of servers.

To add a server to the list, type the name of the computer on which the DeviceLock Enterprise Server is installed. You could type, for instance, the computer’s fully qualified domain name (FQDN), short name or IP address. To add multiple servers, type computer names separated by a semicolon (;).

Individual computer names can be changed or removed from the list. To clear the list, click the **Remove** button.

## Digital Fingerprints Content Groups

Digital Fingerprints content groups implement content inspection using digital fingerprints. Each group of this type references a certain classification of digital fingerprints, and specifies a minimum percentage of fingerprints matching (referred to as threshold) that is required for assigning that classification to the content being inspected.

Content-aware rules can leverage content groups of the Digital Fingerprints type for data analysis based on digital fingerprints. Such rules can be applied to both devices and network protocols, to enable the use of digital fingerprints to control content access permissions, content shadowing, and/or content detection.

Creating a Digital Fingerprints group requires the following steps:

1. Open the dialog box for managing content-aware rules. On how to open this dialog box see [Editing or Deleting Custom Content Groups](#).
2. In the dialog box for managing content-aware rules, under **Content Database**, expand the drop-down list next to **Add Group**, and then click **Digital Fingerprints** in that list.
3. Configure the group settings in the dialog box that appears (see [Dialog box for configuring a Digital Fingerprints group](#)).

Once a Digital Fingerprints group has been created, it can be used along with other content groups when setting up content inspection rules as described earlier in this document, in the section [Content-Aware Rules \(Regular Profile\)](#).

### Dialog box for configuring a Digital Fingerprints group

In the dialog box for configuring a Digital Fingerprints group, the administrator can view or change the following settings:

- **Name** - The name that serves to identify the group.
- **Description** - Optional text that could describe, for example, the purpose of the group.
- **DeviceLock Server** - The name of the computer running DeviceLock Enterprise Server (for example, the fully qualified domain name (FQDN) of that computer). This setting is only used to configure the group, and does not affect applying and processing the rules based on this group. The dialog box gets the list of custom classifications from the server specified in this field. If the DeviceLock Enterprise Servers have no custom classifications or they are not needed for this particular group, then this field can be left blank. As a result, the **Classification level** list does not include any custom classifications and the **Fetch** button is unavailable.
- **Classification level** - The classification of digital fingerprints to be used by this group. Rules that employ this group check submitted information by matching its fingerprints with the fingerprints contained in the classification specified. When the rule detects a sufficient match of the fingerprints, the information is assigned the respective classification level.  
The **Classification level** list allows the administrator to select any built-in classification except "Unclassified". It can be extended to include custom classifications that exist on DeviceLock

Enterprise Server(s). To extend the list, fill in the **DeviceLock Server** field, and then click the **Fetch** button.

---

**Note**

Once the settings are applied and the dialog box is closed, the console preserves the server name specified and custom classifications from that server will be automatically added to the list when opening this dialog box the next time.

---

- **Exact file match** - With this check box selected, the group serves to detect exact matches of files being inspected, with source files of fingerprints from the database. A rule that uses such a group detects a two files match in only case of a match of their checksums. Other elements (hashes) of those files' fingerprints are not compared.

If a file exactly matches a source file that has a non-zero percentage of fingerprint elements attributed to different classifications, then the file is assigned the highest level of those classifications. For example, if the fingerprint of the source file is 10% "Top Secret" and 90% "Unclassified", then the file that exactly matches this source file is considered "Top Secret". As a result, the group may not detect exact file match if the group's classification level is lower than the highest classification level of the fingerprint source file.

If this check box is cleared, the group serves to compare other fingerprint elements (hashes), which enables it to detect partial matches of inspected content with source content of fingerprints from the database. The degree of fingerprint matching that would indicate a partial match of content is determined by the **Threshold** setting.

---

**Note**

When a given group has the **Exact file match** check box selected:

- The group compares the checksum of the file being inspected with the checksums of the source files of all fingerprint versions found in the classification specified.
  - Rules that use this group may skip inspecting fingerprints of files held in archives. For details, see [Inspecting fingerprints within archives](#).
  - An "allow" rule based on such a group takes precedence over "deny" rules (if any), and will allow the transfer of any matching content. An "allow" rule based on a complex group would take precedence in a situation where the logically connected chain of groups that allows the given content includes a group with the **Exact file match** check box selected.
- 

- **Threshold** - The rule triggers if the percentage of information in the inspected content matching the selected classification level exceeds the value that this setting specifies. The percentage of information matching the given classification is determined by assessing how many elements in the fingerprint of the inspected content match the fingerprints of that classification held in the database. More information on this can be found in [How It Works](#) (see [Match percentage](#)).
- **Use only binary fingerprints for password protected documents** - When this check box is selected, the group omits checking text content if it cannot be extracted from the document or archive due to password-protection. A rule that uses such a group checks fingerprints of binary and, if possible, text content. If DeviceLock cannot extract text content, then the rule is limited to



checking binary content.

When this check box is cleared, the group raises an error if it cannot check text content of a password-protected document or archive. In this case, DeviceLock Service does not allow that document or archive due to an error when inspecting its fingerprints.

# Protocols (Regular Profile)

## Overview

DeviceLock allows you to control data that is transferred over different network protocols, thus enhancing protection against unwanted information disclosure and offering additional transport-level security. With the Protocols feature, you can define policies to selectively allow or block data/file transmission via specific protocols as well as shadow copy the transferred data. For flexibility, policies can be defined on a per-user or per-group basis.

DeviceLock recognizes and controls the following protocols:

- **Career Search** - Controls looking for vacancies on job search websites, including the control of files, messages and search requests of users accessing those sites. Controlled are the websites of the following job search providers (including sites in national domains):
  - Avito
  - CareerBuilder
  - College Recruiter
  - craigslist
  - Dice
  - Glassdoor
  - GovernmentJobs
  - HeadHunter.com
  - hh.ru
  - Hired
  - Indeed
  - JobisJob
  - Ladders
  - Mediabistro
  - Monster
  - Rabota.ru
  - Simply Hired
  - SuperJob.ru
  - us.jobs
  - USAJOBS
  - Yandex.Rabota
  - ZipRecruiter
- **File Sharing** - Controls data exchange via Web-based file storage, sharing and synchronization services. The following services are supported:
  - 4shared (including the control of the 4shared app for Windows desktop)
  - Amazon Simple Storage Service (Amazon S3)

- AnonFile
- Box
- Cloud Mail.ru
- Dropbox

---

**Note**

To use the Dropbox application for Windows, a rule that specifies the following hosts for the SSL protocol must be added to the protocols white list:

- \*.dropbox.com
- \*.compute-1.amazonaws.com

For instructions, see [Defining Protocols White List](#).

---

- DropMeFiles
- Easyupload.io
- Files.fm
- freenet.de
- GitHub file sharing service

---

**Note**

To access the GitHub file sharing service using Windows applications such as GitHub Desktop, SmartGit or TortoiseGit, a rule that specifies the host github.com for the SSL protocol must be added to the protocols white list.

For instructions, see [Defining Protocols White List](#).

---

- GMX File Storage
- Gofile.io
- Google Docs / Google Drive

---

**Note**

To use the Backup and Sync from Google application (formerly Google Drive Sync), a rule that specifies the following hosts for the SSL protocol must be added to the protocols white list:

- \*accounts.google.com
- \*www.googleapis.com

For instructions, see [Defining Protocols White List](#).

---

- iCloud
- IDrive
- MagentaCLOUD
- MediaFire

- MEGA (including the control of the MEGAsync app for Windows desktop)

---

**Note**

DeviceLock controls access to the MEGA file sharing service and the uploading of files through that service (outgoing files). The control of incoming files and POST-requests for MEGA is not performed.

---

- OneDrive
- Sendspace
- transfer.sh
- TransFiles.ru
- Uploadfiles.io
- Web.de file sharing service
- WeTransfer
- Yandex.Disk

---

**Note**

To use the Yandex.Disk application for Windows, a rule that specifies the following hosts for the SSL protocol must be added to the protocols white list:

- webdav.yandex.ru
- \*downloader.disk.yandex.ru
- uploader\*.disk.yandex.net
- push.yandex.ru
- \*.storage.yandex.net
- oauth.yandex.ru
- cloud-api.yandex.net

For instructions, see [Defining Protocols White List](#).

---

In addition to controlling file sharing Web services over HTTP, DeviceLock also controls file and data exchange via the Web Distributed Authoring and Versioning (WebDAV) protocol.

Both non-SSL and SSL connections are supported.

- **FTP** (File Transfer Protocol) - The Internet standard protocol for transferring files between computers.  
Both active-mode and passive-mode FTP connections are supported. FTPS (FTP over SSL) is also supported. Both implicit and explicit FTPS connections are supported.
- **HTTP** (Hypertext Transfer Protocol) - An application-level client/server protocol used for data transfer over the World Wide Web.  
Control over HTTP also includes control over data exchange via the Web Distributed Authoring and Versioning (WebDAV) protocol, an extension to HTTP.  
HTTPS (SSL over HTTP) is supported as well.

- **IBM Notes** - A proprietary protocol that IBM Notes uses to communicate with IBM Domino server. DeviceLock supports version 8.5 (December 2008) and later versions (any client-server combinations that Domino / Notes support).
- **ICQ Messenger** - Open System for Communication in Realtime (OSCAR) protocol used by ICQ Instant Messenger.  
Both non-SSL and SSL connections are supported.
- **IRC** (Internet Relay Chat) - An Internet standard protocol that supports interactive, real-time, text-based communications in established “chat rooms” on the Internet by means of IRC servers.  
Both non-SSL and SSL connections are supported.
- **Jabber** - An open, XML-based protocol for instant messaging. Jabber is also known as XMPP, the Extensible Messaging and Presence Protocol.
- **Mail.ru Agent** - An instant messaging program created by Mail.ru.

---

#### Note

SSL connections between Jabber/Mail.ru Agent clients and the server are controlled as generic (non-SSL) connections.

---

- **MAPI** (Messaging Application Programming Interface) - MAPI/RPC (also known as Outlook - Exchange Transport Protocol) is the proprietary protocol that Microsoft Outlook uses to communicate with Microsoft Exchange Server. DeviceLock supports all versions of Outlook (both 32-bit and 64-bit) starting with Outlook 2003. Also supported are all versions of Exchange Server.
- **Skype** - A proprietary voice-over-Internet protocol service and software application. Within this protocol, DeviceLock controls communications through the following applications:
  - Skype version 4.x or later
  - Skype for Business 2015, 2016, or 2019
  - Microsoft Lync 2013
  - Skype Meetings App
  - Skype for Business Web App
  - Skype for Business in Outlook Web App (OWA 365)

---

#### Note

Communications using MSN/Windows Messenger are blocked if any permissions, auditing, shadowing or alert settings are configured for the Skype protocol.

---

- **SMB** (Server Message Block) - A network file sharing protocol.
- **SMTP** (Simple Mail Transfer Protocol) - An Internet standard protocol used for exchanging e-mail messages between SMTP servers on the Internet.  
Extended SMTP (ESMTP) is also supported. Both non-SSL and SSL connections are supported.
- **Social Networks** - Controls communication with social networking sites. The following social networking sites are supported:
  - Disqus
  - Facebook (+API)
  - Google+

- Instagram (including the control of the Instagram app for Windows 10)
- LinkedIn
- LiveInternet.ru
- LiveJournal
- Myspace
- Odnoklassniki.ru
- Pinterest
- Tumblr
- Twitter
- V Kontakte (+API)
- XING.com

---

**Note**

SSL traffic on social networking sites is controlled as generic (non-SSL) traffic.

---

- **Telegram** - Controls the Telegram Desktop and Telegram Web messaging apps, including the Telegram Desktop app for Windows 10.
- **Telnet** - The Internet standard protocol for remote terminal connection service.
- **Torrent** - Controls peer-to-peer (P2P) communications of torrent clients over TCP, UDP or HTTP protocols.
- **Viber** - An instant messaging and voice-over-IP service and software application. DeviceLock supports Windows-based Viber application version 4.x and later.
- **Web Mail** - Controls Web-based mail communication. The following Web-based e-mail services are supported:
  - ABV Mail
  - AOL Mail
  - freenet.de
  - Gmail
  - GMX Mail
  - Hotmail (Outlook.com)
  - iCloud
  - Mail.ru
  - NAVER
  - Outlook Web App (OWA)
  - Rambler Mail
  - T-online.de
  - Web.de
  - Yahoo! Mail
  - Yandex Mail
  - Zimbra

Both non-SSL and SSL connections are supported.

---

**Note**

If the HTTP protocol is not allowed by the protocol permission settings, connection to the Zimbra or Outlook Web App (OWA) mail service may fail despite the Web Mail protocol permission. To prevent failures in this case, add the Zimbra and OWA hosts to the white list for the HTTP protocol. For instructions, see [White List Management Tasks](#).

---

**Note**

Emails sent from Microsoft Outlook via Google Workspace Sync for Microsoft Outlook (GWSMO, formerly G Suite) are controlled according to the Web Mail settings for Gmail.

---

- **Web Search** - Controls the use of websites that provide web-search services, as well as user search requests on those sites. Controlled are the sites of the following web-search providers (including websites in national domains and mobile versions of the websites):
  - Google
  - Yandex
  - Bing
  - Baidu
  - Yahoo
  - Mail.ru
  - Ask.com
  - AOL Search
  - Rambler
  - Wolfram Alpha
  - DuckDuckGo
  - WebCrawler
  - Search.com
  - Wayback Machine
  - Dogpile
  - StartPage
  - Excite
  - NAVER
  - Web.de
- **WhatsApp** - Controls the Web application WhatsApp Web as well as the WhatsApp Desktop application for Windows-based computers.
- **Zoom** - A cloud platform for video and audio conferencing, collaboration, chat, and webinars provided by [Zoom Video Communications \(zoom.us\)](#). Within this protocol, DeviceLock controls the use of the Zoom communication application for Windows-based computers, including connections to Zoom servers, participation in Zoom meetings, and the exchange of messages and files using that application.

---

**Note**

To allow applications with embedded SSL certificates to connect to their servers, the respective hosts should be white-listed for the SSL protocol (see [Managing Protocols White List](#)).

---

Security policies for protocols can be administered by using the DeviceLock Management Console, Service Settings Editor, or DeviceLock Group Policy Manager. The administrator can also use the [Report Permissions/Auditing](#) plug-in from [DeviceLock Enterprise Manager](#) to view or change security policies defined for protocols.

## Protocols Node

The **Protocols** node allows you to access the following functions of DeviceLock:

- Permissions for protocols (see [Managing Permissions for Protocols](#), [Managing Offline Permissions for Protocols](#))
- Auditing, shadowing and alerts for protocols (see [Managing Audit, Shadowing and Alerts for Protocols](#), [Managing Offline Audit, Shadowing and Alerts for Protocols](#))
- Protocols white list (see [Managing Protocols White List](#), [Managing Offline Protocols White List](#))
- Basic IP firewall (see [Managing Basic IP Firewall](#), [Managing Offline IP Firewall](#))
- Content-aware rules for protocols (see [Rules for Protocols](#), [Defining Rules for Protocols](#), [Managing Offline Content-Aware Rules for Protocols](#))
- Security settings for protocols (see [Managing Security Settings for Protocols](#), [Managing Offline Security Settings for Protocols](#))

The shortcut menu on the **Protocols** node provides the following commands:

- **Undefine NetworkLock Policy** - Resets all parameters specific to NetworkLock to the unconfigured state.
- **Undefine ContentLock Policy** - Resets parameters specific to ContentLock (all content-aware rules except those based on file types) to the unconfigured state.

### Recommendations

After configuring protocol access permissions, a “Server timeout” error may occur when trying to connect to some secure websites. This issue is because DeviceLock encrypts SSL traffic by using its own certificate, while some web sites/applications can only work with their predefined certificate.

To resolve the issue, add a white list rule for the SSL protocol that specifies the domain names or IP addresses, and ports used by those web site/application servers (for rule configuration instructions, see [Defining Protocols White List](#)).

In the case of a web application, you must first find out its connection servers. This can be done with the TCP View tool, available at [docs.microsoft.com/sysinternals/downloads/tcpview](https://docs.microsoft.com/sysinternals/downloads/tcpview). Some applications use server pools with reserved IP ranges, making it difficult to configure white list rules. In this case, we recommend contacting the application support for a complete list of IP addresses (ranges) in use.



# Managing Permissions for Protocols

To govern the exchange of information at the transport level, configure access to communications protocols by setting appropriate permissions. These permissions specify who can gain access to which protocols and what level of access users have. Permissions can be set on a per-user or per-group basis. Description of access rights for each protocol is given in the [Access Rights](#) section.

When you select the **Protocols > Permissions** node in the console tree, the details pane [lists the protocols](#) for which you can define permissions (see [Permission Management Tasks](#)).

## Access Rights

The following sections cover access rights available for permissions associated with protocols:

- [Career Search](#)
- [File Sharing](#)
- [FTP](#)
- [HTTP](#)
- [IBM Notes](#)
- [ICQ Messenger](#)
- [IRC](#)
- [Jabber](#)
- [Mail.ru Agent](#)
- [MAPI](#)
- [Skype](#)
- [SMB](#)
- [SMTP](#)
- [Social Networks](#)
- [Telegram](#)
- [Telnet](#)
- [Torrent](#)
- [Viber](#)
- [Web Mail](#)
- [Web Search](#)
- [WhatsApp](#)
- [Zoom](#)

## Career Search

Access rights applicable to the Career Search protocol:

- **Generic: Send/Receive Data** - The right to access, sign in and browse job search sites.
- **Generic: Search** - The right to search for vacancies on job search sites.

- **Generic: Outgoing Messages** - The right to send messages and to submit résumé and other web-form data on job search sites.
- **Generic: Outgoing Files** - The right to upload files to job search sites.

## File Sharing

Access rights applicable to the File Sharing protocol:

- **Generic: Send/Receive Data** - The right to access a file sharing site, to browse its contents and to download files.
- **Generic: POST Requests** - The right to submit Web form data, such as user comments to specific files. This right does not control the login information entered into the user name and password form.
- **Generic: Outgoing Files** - The right to upload files to a file sharing site.
- **SSL: Send/Receive Data** - The right to access a file sharing site, to browse its contents and to download files using SSL.
- **SSL: POST Requests** - The right to submit Web form data, such as user comments to specific files using SSL. This right does not control the login information entered into the user name and password form.
- **SSL: Outgoing Files** - The right to upload files to a file sharing site using SSL.

---

### Note

The POST Requests access right for the File Sharing protocol, when applied to the iCloud service, controls whether a user can upload non-file data (Mail, Notes, Calendar, Contacts, Reminders) to iCloud. A similar right is used to enable the auditing and shadow copying of non-file data the user uploads to iCloud.

---

## FTP

Access rights applicable to the FTP protocol:

- **Generic: Send/Receive Data** - The right to connect to an FTP server, send and receive protocol data, download files from an FTP server.
- **Generic: Outgoing Files** - The right to upload files to an FTP server.
- **SSL: Send/Receive Data** - The right to connect to an FTP server, send and receive protocol data, download files from an FTP server using FTPS.
- **SSL: Outgoing Files** - The right to upload files to an FTP server using FTPS.

## HTTP

Access rights applicable to the HTTP protocol:

- **Generic: Send/Receive Data** - The right to connect to a Web server, send and receive protocol data, web pages and objects on web pages (such as scripts, Flash files, JPEG, PNG, and GIF images, etc.), and download files.
- **Generic: POST Requests** - The right to submit Web form data to a Web server using HTTP.

- **Generic: Outgoing Files** - The right to upload files to a Web server using HTTP.
- **SSL: Send/Receive Data** - The right to connect to a Web server, send and receive protocol data, web pages and objects on web pages (such as scripts, Flash files, JPEG, PNG, and GIF images, etc.), and download files using HTTPS.
- **SSL: POST Requests** - The right to submit Web form data to a Web server using HTTPS.
- **SSL: Outgoing Files** - The right to upload files to a Web server using HTTPS.

## IBM Notes

Access rights applicable to the IBM Notes protocol:

- **Generic: Send/Receive Data** - The right to connect the IBM Notes client to IBM Domino server and read e-mail.
- **Generic: Outgoing Messages** - The right to send e-mail messages without attachments from the IBM Notes client to IBM Domino server.
- **Generic: Outgoing Files** - The right to send e-mail attachments from the IBM Notes client to IBM Domino server.

## ICQ Messenger

Access rights applicable to the ICQ Messenger protocol:

- **Generic: Send/Receive Data, Outgoing Messages** - The right to connect to the ICQ Messenger server and to send and receive instant messages and receive files.
- **Generic: Outgoing Files** - The right to send files.
- **SSL: Send/Receive Data, Outgoing Messages** - The right to connect to the ICQ Messenger server and to send and receive instant messages and receive files using SSL.
- **SSL: Outgoing Files** - The right to send files using SSL.

## IRC

Access rights applicable to the IRC protocol:

- **Generic: Send/Receive Data, Outgoing Messages** - The right to connect to an IRC server and to send and receive instant messages and receive files.
- **Generic: Outgoing Files** - The right to send files.
- **SSL: Send/Receive Data, Outgoing Messages** - The right to connect to an IRC server and to send and receive instant messages and receive files using SSL.
- **SSL: Outgoing Files** - The right to send files using SSL.

## Jabber

Access rights applicable to the Jabber protocol:

- **Generic: Send/Receive Data, Outgoing Messages** - The right to connect to a Jabber server and to send and receive instant messages and receive files.

- **Generic: Outgoing Files** - The right to send files.

## Mail.ru Agent

Access rights applicable to the Mail.ru Agent protocol:

- **Generic: Send/Receive Data, Outgoing Messages** - The right to connect Mail.ru Agent to the Mail.ru server and to send and receive instant messages and receive files.
- **Generic: Outgoing Files** - The right to send files.

## MAPI

Access rights applicable to the MAPI protocol:

- **Generic: Send/Receive Data** - The right to connect the Outlook client to Microsoft Exchange Server and read e-mail.
- **Generic: Outgoing Messages** - The right to send e-mail messages without attachments from the Outlook client to Microsoft Exchange Server.
- **Generic: Outgoing Files** - The right to send e-mail attachments from the Outlook client to Microsoft Exchange Server.

---

### Note

By default, the access rights for the MAPI protocol also apply to draft folder messages that Outlook saves to the Exchange Server, and to messages being sent to the Exchange Server from e-mail message export files (.msg files) or other (external) mailboxes. This behavior can be changed by disabling the **Intercept draft MAPI messages** and/or **Intercept moved MAPI messages** setting (see [Managing Security Settings for Protocols](#)).

---

## Skype

Access rights applicable to the Skype protocol:

- **Generic: Send/Receive Data** - The right to connect to the Skype server and receive instant messages and files.
- **Generic: Incoming Calls** - The right to receive calls.
- **Generic: Outgoing Calls** - The right to make calls.
- **Generic: Outgoing Messages** - The right to send instant messages.
- **Generic: Outgoing Files** - The right to send files.

## SMB

Access rights applicable to the SMB protocol:

- **Generic: Send/Receive Data** - The right to connect to, and browse shared network folders on SMB servers.
- **Generic: Incoming Files** - The right to download files from SMB servers to the computer running DeviceLock Service, as well as to upload files to shared network folders on that computer.

- **Generic: Outgoing Files** - The right to upload files from the computer running DeviceLock Service to SMB servers, as well as to download files from shared network folders on that computer.

---

#### Note

- Access rights for the SMB protocol have no effect on the operation of registering shared network printers with computers under the control of the DeviceLock Service. Even if DeviceLock is configured to block data exchange via the SMB protocol, this does not prevent the operating system from downloading the network printer driver. However, in this case DeviceLock will not allow the user to download the network printer driver by hand.
  - Access rights for the SMB protocol have no effect on the operation of Group Policy on computers in an Active Directory environment. Even if DeviceLock is configured to block data exchange via the SMB protocol, this does not apply to Group Policy data exchange. Group Policy settings are updated and applied regardless of the access rights for the SMB protocol.
- 

## SMTP

Access rights applicable to the SMTP protocol:

- **Generic: Send/Receive Data** - The right to connect to an SMTP server and to send and receive protocol data.
- **Generic: Outgoing Messages** - The right to send e-mail messages without attachments.
- **Generic: Outgoing Files** - The right to send e-mail attachments.
- **SSL: Send/Receive Data** - The right to connect to an SMTP server and to send and receive protocol data using SSL.
- **SSL: Outgoing Messages** - The right to send e-mail messages without attachments using SSL.
- **SSL: Outgoing Files** - The right to send e-mail attachments using SSL.

## Social Networks

Access rights applicable to Social Networks protocol:

- **Generic: Send/Receive Data** - The right to have view access to a social networking site.
- **Generic: Outgoing Messages** - The right to send messages, comments, posts, etc.
- **Generic: Outgoing Files** - The right to upload media and file content to a social networking site.

## Telegram

Access rights applicable to the Telegram protocol:

- **Generic: Send/Receive Data** - The right to use Telegram Desktop. Permits access to Telegram servers.
- **Generic: Web Send/Receive Data** - The right to use Telegram Web. Permits access to the Telegram Web host (web.telegram.org).

## Telnet

Access rights applicable to the Telnet protocol:

- **Generic: Send/Receive Data** - The right to connect to a Telnet server and to send and receive protocol data.

## Torrent

Access rights applicable to the Torrent protocol:

- **Generic: Send/Receive Data** - The right to connect to remote hosts.

## Viber

Access rights applicable to the Viber protocol:

- **Generic: Send/Receive Data, Outgoing Messages** - The right to connect to the Viber server, send and receive instant messages, and receive files.
- **Generic: Outgoing Files** - The right to send files.

## Web Mail

Access rights applicable to the Web Mail protocol:

- **Generic: Send/Receive Data** - The right to access Webmail and read e-mail.
- **Generic: Outgoing Messages** - The right to send e-mail messages without attachments.
- **Generic: Outgoing Files** - The right to send e-mail attachments.
- **SSL: Send/Receive Data** - The right to access Webmail and read e-mail using SSL.
- **SSL: Outgoing Messages** - The right to send e-mail messages without attachments using SSL.
- **SSL: Outgoing Files** - The right to send e-mail attachments using SSL.

## Web Search

Access rights applicable to the Web Search protocol:

- **Generic: Search** - The right to perform web searches using requests on web search sites or by entering URL-s containing search requests into the web browser's address string.

## WhatsApp

Access rights applicable to the WhatsApp protocol:

- **Generic: Send/Receive Data** - The right to use WhatsApp Desktop on Windows-based computers.
- **Generic: Web Send/Receive Data** - The right to use WhatsApp in Web-browsers on Windows-based computers.

## Zoom

Access rights applicable to the Zoom protocol:

- **Generic: Send/Receive Data** - The right to connect to the Zoom server, use the Zoom application for video and audio conferencing and webinars, and receive messages and files via the Zoom application.
- **Generic: Outgoing Calls** - The right to participate in Zoom meetings.
- **Generic: Outgoing Messages** - The right to send instant messages from the Zoom application.
- **Generic: Outgoing Files** - The right to send files from the Zoom application.

## Default Permissions

The **Permissions** dialog box provides the option to set default permissions to access protocols. These permissions are assigned to the Administrators and Everyone groups, and, in the case of the SMB protocol, to the SYSTEM account. The following table lists the default permissions for each protocol.

Account/ Protocol	Administrators	Everyone
Career Search	Generic: Send/Receive Data, Search, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Search, Outgoing Messages
File Sharing	Generic: Send/Receive Data, POST Requests, Outgoing Files SSL: Send/Receive Data, POST Requests, Outgoing Files	Generic: Send/Receive Data, POST Requests SSL: Send/Receive Data, POST Requests
FTP	Generic: Send/Receive Data, Outgoing Files SSL: Send/Receive Data, Outgoing Files	Generic: Send/Receive Data SSL: Send/Receive Data
HTTP	Generic: Send/Receive Data, POST Requests, Outgoing Files SSL: Send/Receive Data, POST Requests, Outgoing Files	Generic: Send/Receive Data, POST Requests SSL: Send/Receive Data, POST Requests
IBM Notes	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
ICQ Messenger	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages SSL: Send/Receive Data, Outgoing Messages
IRC	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages

	SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	SSL: Send/Receive Data, Outgoing Messages
Jabber	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Mail.ru Agent	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
MAPI	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Skype	Generic: Send/Receive Data, Incoming Calls, Outgoing Messages, Outgoing Files, Outgoing Calls	Generic: Send/Receive Data, Incoming Calls, Outgoing Messages, Outgoing Calls
SMB	Generic: Send/Receive Data, Outgoing Files, Incoming Files  <b>Note:</b> In the case of the SMB protocol, these default permissions are also assigned to the SYSTEM account.	Generic: Send/Receive Data
SMTP	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
	SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	SSL: Send/Receive Data, Outgoing Messages
Social Networks	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Telegram	Generic: Send/Receive Data, Web Send/Receive Data	Generic: Send/Receive Data, Web Send/Receive Data
Telnet	Generic: Send/Receive Data	Generic: Send/Receive Data
Torrent	Generic: Send/Receive Data	Generic: Send/Receive Data
Viber	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
Web Mail	Generic: Send/Receive Data, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Messages
	SSL: Send/Receive Data, Outgoing Messages, Outgoing Files	SSL: Send/Receive Data, Outgoing Messages
Web Search	Generic: Search	Generic: Search
WhatsApp	Generic: Send/Receive Data, Web Send/Receive Data	Generic: Send/Receive Data, Web Send/Receive Data
Zoom	Generic: Send/Receive Data, Outgoing Calls, Outgoing Messages, Outgoing Files	Generic: Send/Receive Data, Outgoing Calls, Outgoing Messages



## Permission Management Tasks

Managing online (regular) permissions for protocols involves the following tasks:

- [Setting and editing permissions](#)
- [Undefining permissions](#)

---

### Note

You can define different online vs. offline permissions on protocols for the same user or sets of users. Online permissions (Regular Profile) apply to client computers that are working online. Offline permissions (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define offline permissions for protocols, see [Managing Offline Permissions for Protocols](#).

---

Online permissions for a protocol can have one of the following states:

- **Configured** - Different accounts are assigned different permissions for the protocol.
- **Full Access** - All accounts have full access to the protocol.  
This state shows up, for example, when permissions are set only for the “Everyone” account so that it has full access to the protocol.
- **No Access** - No accounts have access to the protocol.  
This state shows up, for example, when the “Everyone” account is explicitly denied any access to the protocol, or permissions are not set for any accounts. Note that the denial for the “Everyone” account overrides any permissions for other accounts.
- **Not Configured** - No permission settings are specified for the protocol.

## Setting and editing permissions


### *To set and edit permissions*

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.

3. Under **Protocols**, select **Permissions**.

*When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions. In the details pane, you can also view the current state of online (regular) permissions for each protocol in the Regular column.*

4. In the details pane, do one of the following:

- Right-click the protocol for which you want to set or edit permissions, and then click **Set Permissions**.
- OR -
- Select the protocol for which you want to set or edit permissions, and then click **Set Permissions**  on the toolbar.

*You can select multiple protocols for which you want to set the same permissions by holding down the SHIFT key or the CTRL key while clicking them.*

---

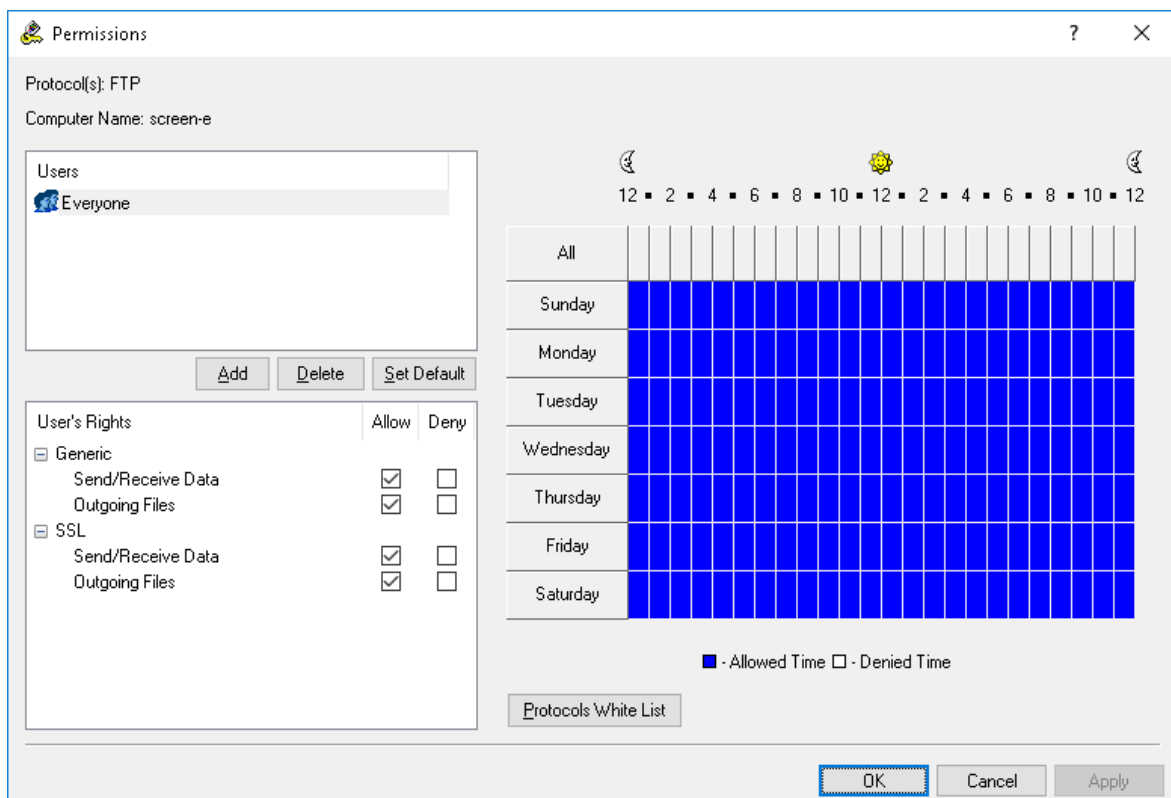
#### **Note**

When selecting several protocols with different access rights, consider the following:

- The **Permissions** dialog box displays only those access rights that are common to all selected protocols. When you allow or deny any of the displayed access rights, you configure access to each of the selected protocols.
- Some access rights depend on other rights. If you grant a right that requires another right, the required right is granted automatically. For example, if you grant only the **Generic: Outgoing Files** right for the Social Networks and Web Mail protocols, the following rights are granted automatically: **Generic: Send/Receive Data**, **Generic: Outgoing Messages**, **Generic: Outgoing Files**.

---

*The Permissions dialog box appears.*



5. In the **Permissions** dialog box, do the following:

**To set the default permissions**

- In the upper-left pane of the dialog box, under **Users**, click **Set Default**.  
The default permissions are assigned to the Administrators and Everyone groups. For further details, see [Default Permissions](#).

**To set permissions for an additional user or group**

- In the upper-left pane of the dialog box, under **Users**, click **Add**.
- In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.  
*The added users and groups appear in the upper-left pane of the Permissions dialog box.*
- In the upper-left pane of the **Permissions** dialog box, under **Users**, select the user or group.  
*To select multiple users or groups, hold down the SHIFT or CTRL key while clicking them.*
- In the lower-left pane of the **Permissions** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate rights (see [Access Rights](#)).  
*In the right pane of the Permissions dialog box, you can set day and time restrictions that narrow user access to the specified protocol(s). Use the left mouse button to select days and hours when the selected user or group will have access to the specified protocol(s). Use the right mouse button to mark days and hours when the selected user or group will not have access to the specified protocol(s).*

**To change permissions for an existing user or group**

- In the upper-left pane of the dialog box, under **Users**, select the user or group.
- In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to

directly allow or deny the appropriate access rights.

**To remove an existing user or group and permissions**

- In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

**To set, view, or change Protocols White List rules for this protocol**

- Click the **Protocols White List** button. For further details, see [Managing Protocols White List](#).

**To set, view, or change Security Settings for the MAPI protocol**

- Click the **Security Settings** button. For further details, see [Managing Security Settings for Protocols](#).

---

**Note**

The **Permissions** dialog box displays the **Security Settings** button only when managing permissions for the MAPI protocol. For other protocols, this button is not available.

---

6. Click **OK** or **Apply**.

## Undefining permissions

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent some or all of the previously set permissions for protocols from being applied to a specific group of client computers. To do so, you need to return the previously set permissions to the unconfigured state. All undefined DeviceLock Service settings are ignored by client computers.

**To undefine permissions**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.  
*When you select Permissions in the console tree, the details pane lists the protocols for which permissions can be set.*
4. In the details pane, right-click the protocol, and then click **Undefine**.  
*You can use the following steps to undefine permissions for multiple protocols at a time:*
  - a. In the details pane, click protocols while holding down the SHIFT or CTRL key.
  - b. Right-click the selection, and then click **Undefine**.

# Managing Audit, Shadowing and Alerts for Protocols

DeviceLock provides the capability to audit and shadow copy data/file transfers via different protocols. Auditing and shadow copying are used to monitor and record security-critical data transfer operations. Regular analysis of log data is an effective way to detect and trace misuse of sensitive information and data breach incidents caused by data loss or theft.

When you select the **Protocols > Auditing, Shadowing & Alerts** node in the console tree, the details pane [lists the protocols](#) for which you can define audit and shadow copy rules (see [Auditing, Shadowing and Alerts Management Tasks](#)). Using this node you can also enable alerts that are sent when a specific user attempts to access a specific protocol (see [Enabling alerts](#)).

For auditing and shadow copying at the transport level, DeviceLock uses two types of logging: Audit Logs and Shadow Logs. The Audit Log is used to audit access to protocols and track what individual users do. Audit data can be written to the Windows Event Log, to the DeviceLock proprietary log, or both. It is also possible to send audit data to a syslog server. To specify where to store audit data, set the [Audit log type](#) parameter in [Service Options](#). To view audit data, use either DeviceLock Service Audit Log Viewer (see [Audit Log Viewer \(Service\)](#)) or DeviceLock Enterprise Server Audit Log Viewer (see [Audit Log Viewer \(Server\)](#)).

The Shadow Log is used to store a full copy of data/files transferred via specified protocols. To view shadow log data, use either DeviceLock Service Shadow Log Viewer (see [Shadow Log Viewer \(Service\)](#)) or DeviceLock Enterprise Server Shadow Log Viewer (see [Shadow Log Viewer \(Server\)](#)).

Auditing and shadow copying of the data transferred via specified protocols are enabled by defining audit and shadowing rules. Each rule associated with a protocol specifies users or groups the rule applies to and appropriate audit/shadowing rights which determine which user actions to audit/shadow copy.

Audit events logged include a variety of information such as the event type, the date and time of the event, the associated protocol, the user associated with this event, process information and event-specific information.

---

## Note

When using shadow copying, keep in mind the following:

- If data transmission is blocked by permissions, a shadow copy of this data is not created. In this case DeviceLock blocks the transmission of data before it is captured. Exception: If data is being inspected by Content-Aware Rules, then DeviceLock creates the shadow copy even if permissions block the transmission of that data.
- 

## Audit and Shadowing Rights

The following sections provide summary information on audit and shadowing rights that can be specified in rules along with a description of event-specific data that is written to the log:

- Career Search
- File Sharing
- FTP
- HTTP
- IBM Notes
- ICQ Messenger
- IRC
- Jabber
- Mail.ru Agent
- MAPI
- Skype
- SMB
- SMTP
- Social Networks
- Telegram
- Telnet
- Torrent
- Viber
- Web Mail
- Web Search
- WhatsApp
- Zoom

## Career Search

Audit and shadowing rights applicable to the Career Search protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to a job search site.  
*The Connection action, the IP address along with the port number and the name of the webhost, and the name of the protocol are written to the log. If the IP address cannot be resolved to a webhost name, the name is not written to the log.*
- **Audit: Search** - Enables the auditing of user attempts to submit a search request for vacancies on a job search site.  
*The Search action, the name of the job search service along with the search string entered by the user, the IP address with the port number and the name of the webhost, and the name of the protocol are written to the log.*
- **Audit: Outgoing Messages** - Enables the auditing of user attempts to send messages and to submit résumé and other web-form data on a job search site.  
*The Outgoing Message action and information to identify the sent content (<site\_name>: <content\_name>) are written to the log. Recipient IDs are only written to the log upon user attempts to send messages.*

- **Audit: Outgoing Files** - Enables the auditing of user attempts to upload a file to a job search site. *The Outgoing File action and information to identify the uploaded file (<site\_name>: <file\_name>) are written to the log.*
- **Shadowing: Search** - Enables the shadow copying of the vacancy search requests entered by the user on job search sites. *A shadow copy of each search request is written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of messages sent as well as résumé and other web-form data submitted to job search sites. *Shadow copies of sent messages, submitted résumé and other web-form data are written to the log.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of files uploaded to job search sites. *Shadow copies of uploaded files are written to the log.*

## File Sharing

Audit and shadowing rights applicable to the File Sharing protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to a file sharing site. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to download a file from a file sharing site. *The Incoming File action, the download link, the IP address with the port number and the name of the host, the name of the protocol are written to the log.*
- **Audit: POST Requests** - Enables the auditing of user attempts to submit Web form data, such as user comments to specific files. *The POST Request action, the name of the file storage, sharing and synchronization service, the IP address with the port number and the name of the host, the name of the protocol are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to upload a file to a file sharing site. *The Outgoing File action, the name of the file, the IP address with the port number and the name of the host, the name of the protocol are written to the log.*
- **Shadowing: Incoming Files** - Enables the shadow copying of files downloaded from a file sharing site. *Shadow copies of downloaded files are written to the log.*
- **Shadowing: POST Requests** - Enables the shadow copying of data (user comments to specific files) entered into Web forms. *Shadow copies of data entered into Web forms are written to the log.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of files uploaded to a file sharing site. *Shadow copies of uploaded files are written to the log.*

---

## Note

The POST Requests right for the File Sharing protocol, when applied to the iCloud service, enables the auditing and shadow copying of non-file data (Mail, Notes, Calendar, Contacts, Reminders). Audit records of upload attempts and shadow copies of that data are stored as Outgoing Messages.

---

## FTP

Audit and shadowing rights applicable to the FTP protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to an FTP site.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to download a file from an FTP site.  
*The Incoming File action, the absolute path and complete name of the file (for example, ftp://myftp/myfile.doc), the IP address with the port number and the name of the host are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to upload a file to an FTP site.  
*The Outgoing File action, the absolute path and complete name of the file (for example, ftp://myftp/myfile.doc), the IP address with the port number and the name of the host are written to the log.*
- **Shadowing: Incoming Files** - Enables the shadow copying of files downloaded from an FTP site.  
*Shadow copies of downloaded files are written to the log.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of files uploaded to an FTP site.  
*Shadow copies of uploaded files are written to the log.*

## HTTP

Audit and shadowing rights applicable to the HTTP protocol:

- **Audit: Connection** - Enables the auditing of allowed and denied user attempts to open a web page.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*

---

## Note

When this right is enabled, numerous Connection events are recorded in the Audit Log each time a user attempts to open a web page. This happens because a web page often requests resources (such as images, scripts, etc.) from other hosts.

---

- **Audit: Incoming Data** - Enables the auditing of web pages and objects on web pages.



*The Incoming Data action, the URL of the web page and objects on the web page (e.g., absolute path with URL to request parameters http://domain/path), the IP address with the port number and the name of the host are written to the log.*

- **Audit: Incoming Files** - Enables the auditing of user attempts to download a file from a Web site.  
*The Incoming File action, the absolute path and complete name of the file (for example, http://domain/path/myfile.doc), the IP address with the port number and the name of the host are written to the log.*
- **Audit: Outgoing Data** - The Outgoing Data content type contains no data.  
*The Outgoing Data action, the URL of the web page and objects on the web page (e.g., absolute path with URL to request parameters http://domain/path), the IP address with the port number and the name of the host are written to the log.*
- **Audit: POST Requests** - Enables the auditing of user attempts to submit Web form data to a Web site.  
*The POST Request action and the URL of the script that sent the POST request (e.g., absolute path with URL to request parameters http://domain/path) are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to upload a file to a Web site.  
*The Outgoing File action, the name of the file and the name of the server that receives the file (for example, http://server/file.doc), the IP address with the port number and the name of the host are written to the log.*
- **Shadowing: Incoming Data** - Enables the shadow copying of web pages and objects on web pages.  
*Shadow copies of web pages and their constituent components are written to the log.*
- **Shadowing: Incoming Files** - Enables the shadow copying of files downloaded from a Web site.  
*Shadow copies of downloaded files are written to the log.*
- **Shadowing: Outgoing Data** - This right has no impact on the shadow copying.
- **Shadowing: POST Requests** - Enables the shadow copying of data entered into Web forms.  
*Shadow copies of data entered into Web forms are written to the log.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of files uploaded to a Web site.  
*Shadow copies of uploaded files are written to the log.*

## IBM Notes

Audit and shadowing rights applicable to the IBM Notes protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect the IBM Notes client to IBM Domino server.  
*The Connection action and the IP address or the name of the host are written to the log. A successful connection to the IBM Domino Server can generate several Connection events.*
- **Audit: Incoming Messages, Incoming Files** - Enables the auditing of user attempts to receive an e-mail message with or without attachments from IBM Domino server to the IBM Notes client.  
*The Incoming Message action, the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender => recipient1, recipient2).*

- **Audit: Outgoing Messages, Outgoing Files** - Enables the auditing of user attempts to send an e-mail message with or without attachments from the IBM Notes client to IBM Domino server.  
*The Outgoing Message action, the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender => recipient1, recipient2).*  
*The number of attachments is always written to the Audit Log.*
- **Shadowing: Incoming Messages, Incoming Files** - Enables the shadow copying of received e-mail messages with or without attachments.  
*Shadow copies of received e-mail messages with or without attachments are written to the log as .eml files. You can, for example, open .eml files in Microsoft Outlook Express, in Windows Mail, and in Mozilla Thunderbird.*
- **Shadowing: Outgoing Messages, Outgoing Files** - Enables the shadow copying of sent e-mail messages with or without attachments.  
*Shadow copies of sent e-mail messages with or without attachments are written to the log as .eml files. These files can be opened, for example, in Microsoft Outlook Express, Windows Mail, or Mozilla Thunderbird.*  
*The number of attachments is always written to the Shadow Log.*

## ICQ Messenger

Audit and shadowing rights applicable to the ICQ Messenger protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to the ICQ Messenger server.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
- **Audit: Incoming Messages, Outgoing Messages** - Enables the auditing of user attempts to send and receive instant messages.  
*The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant precedes the ID of a remote participant.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file.  
*The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file.  
*The Outgoing File action and the name of the file are written to the log.*
- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages.  
*Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files.  
*Shadow copies of received files are written to the log.*

- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages.  
*Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files.  
*Shadow copies of sent files are written to the log.*

## IRC

Audit and shadowing rights applicable to the IRC protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to an IRC server.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
- **Audit: Incoming Messages, Outgoing Messages** - Enables the auditing of user attempts to send and receive instant messages.  
*The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant precedes the ID of a remote participant.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file.  
*The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file.  
*The Outgoing File action and the name of the file are written to the log.*
- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages.  
*Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files.  
*Shadow copies of received files are written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages.  
*Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files.  
*Shadow copies of sent files are written to the log.*

## Jabber

Audit and shadowing rights applicable to the Jabber protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to a Jabber server.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
- **Audit: Incoming Messages, Outgoing Messages** - Enables the auditing of user attempts to send and receive instant messages.  
*The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant precedes the ID of a remote participant.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file.  
*The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file.  
*The Outgoing File action and the name of the file are written to the log.*
- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages.  
*Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files.  
*Shadow copies of received files are written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages.  
*Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files.  
*Shadow copies of sent files are written to the log.*

## Mail.ru Agent

Audit and shadowing rights applicable to the Mail.ru Agent protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect Mail.ru Agent to the Mail.ru server.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
- **Audit: Incoming Messages, Outgoing Messages** - Enables the auditing of user attempts to send and receive instant messages.  
*The Chat action, IDs of all IM participants, the IP address with the port number and the name of the host are written to the log. The ID of the local participant precedes the ID of a remote participant.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file.  
*The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file.  
*The Outgoing File action and the name of the file are written to the log.*

- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages. *Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files. *Shadow copies of received files are written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user quits the instant messenger. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files. *Shadow copies of sent files are written to the log.*

## MAPI

Audit and shadowing rights applicable to the MAPI protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect the Outlook client to Microsoft Exchange Server. *The Connection action and the IP address or the name of the host are written to the log. A successful connection to the Microsoft Exchange Server can generate several Connection events.*
- **Audit: Incoming Messages, Incoming Files** - Enables the auditing of user attempts to receive an e-mail message with or without attachments from Microsoft Exchange Server to the Outlook client. *The Incoming Message action, the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender => recipient1, recipient2).*
- **Audit: Outgoing Messages, Outgoing Files** - Enables the auditing of user attempts to send an e-mail message with or without attachments from the Outlook client to Microsoft Exchange Server. *The Outgoing Message action, the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender => recipient1, recipient2).*  
*The number of attachments is always written to the Audit Log.*
- **Shadowing: Incoming Messages, Incoming Files** - Enables the shadow copying of received e-mail messages with or without attachments. *Shadow copies of received e-mail messages with or without attachments are written to the log as .eml files. These files can be opened, for example, in Microsoft Outlook Express, Windows Mail, or Mozilla Thunderbird.*
- **Shadowing: Outgoing Messages, Outgoing Files** - Enables the shadow copying of sent e-mail messages with or without attachments.

*Shadow copies of sent e-mail messages with or without attachments are written to the log as .eml files. These files can be opened, for example, in Microsoft Outlook Express, Windows Mail, or Mozilla Thunderbird.*

*The number of attachments is always written to the Shadow Log.*

---

#### Note

- When trying to open a .eml file from the Shadow Log, it may appear that the file cannot be opened by using Outlook 2007. For instructions on how to resolve this issue, see Microsoft's article at [support.microsoft.com/kb/956693](https://support.microsoft.com/kb/956693).
  - The audit and shadowing rights for the MAPI protocol also apply to the drafts of the messages not sent from Outlook to Exchange Server. Thus, if the Outlook user has the right to send messages, DeviceLock would log the audit event and/or create the shadow copy for the saved message draft when the user closes Outlook without sending the message. If the user does not have that right, the audit event and/or shadow copy would be created when saving the message draft in Outlook.
- 

## Skype

Audit and shadowing rights applicable to the Skype protocol:

- **Audit: Connection** - Enables the auditing of user attempts to sign in to a Skype account.  
*The Connection action is written to the log.*
- **Audit: Incoming Calls** - Enables the auditing of user attempts to receive calls.  
*The Incoming Call action and Skype names of all call participants are written to the log. The Skype name of the local participant precedes the Skype name of a remote participant.*
- **Audit: Incoming Messages** - Enables the auditing of user attempts to receive instant messages.  
*The Chat action and Skype names of all IM participants are written to the log. The Skype name of the local participant precedes the Skype name of a remote participant.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file.  
*The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Calls** - Enables the auditing of user attempts to make calls.  
*The Outgoing Call action and Skype names of all call participants are written to the log. The Skype name of the local participant precedes the Skype name of a remote participant.*
- **Audit: Outgoing Messages** - Enables the auditing of user attempts to send instant messages.  
*The Chat action and Skype names of all IM participants are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file.  
*The Outgoing File action and the name of the file are written to the log.*
- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages.  
*Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Skype. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files.  
*Shadow copies of received files are written to the log.*



- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Skype. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files. *Shadow copies of sent files are written to the log.*

## SMB

Audit and shadowing rights applicable to the SMB protocol:

- **Audit: Connection** - Enables the auditing of user attempts to access an SMB server. Also enables the auditing of attempts of other computers to gain access to shared network folders located on the computer running DeviceLock Service. *The following is written to the log: the Connection action and either the name or IP address of the SMB server to which access was requested, or the name or IP address of the computer that requested access to the computer running DeviceLock Service. To prevent the log cluttering by excessive number of connection-related records, only the first connection with the given SMB server or external computer is logged.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to download files from an SMB server. Also enables the auditing of attempts of other computers to upload files to shared network folders located on the computer running DeviceLock Service. *The Incoming File action and the name of each incoming file are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to upload files to an SMB server. Also enables the auditing of attempts of other computers to download files from shared network folders located on the computer running DeviceLock Service. *The Outgoing File action and the name of each outgoing file are written to the log.*
- **Shadowing: Incoming Files** - Enables the shadow copying of files downloaded from SMB servers. Also enables the shadow copying of files uploaded by other computers to shared network folders located on the computer running DeviceLock Service. *A shadow copy of each incoming file is written to the log.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of files uploaded to SMB servers. Also enables the shadow copying of files downloaded by other computers from shared network folders located on the computer running DeviceLock Service. *A shadow copy of each outgoing file is written to the log.*

## SMTP

Audit and shadowing rights applicable to the SMTP protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to an SMTP server. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*

- **Audit: Outgoing Messages, Outgoing Files** - Enables the auditing of user attempts to send an e-mail message with or without attachments.

*The Outgoing Message action, the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender => recipient1, recipient2).*

*The number of attachments is always written to the Audit Log.*

- **Shadowing: Outgoing Messages, Outgoing Files** - Enables the shadow copying of sent e-mail messages with or without attachments.  
*Shadow copies of sent e-mail messages with or without attachments are written to the log as .eml files. You can, for example, open .eml files in Microsoft Outlook Express, in Windows Mail, and in Mozilla Thunderbird.*  
*The number of attachments is always written to the Shadow Log.*

## Social Networks

Audit and shadowing rights applicable to the Social Networks protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to a social networking site.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
- **Audit: Outgoing Messages** - Enables the auditing of user attempts to send messages, comments, posts, etc.  
*The Outgoing Message action and information to identify the sent content (<site\_name>: <content\_name>\_<Recipient ID>) are written to the log. Recipient IDs, in a numeric form, are only written to the log upon users attempt to send messages.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to upload media and file content to a social networking site.  
*The Outgoing File action and information to help identify the uploaded file (<site\_name>: <file\_name>) are written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent messages, comments, posts, etc.  
*Shadow copies of sent messages, comments, etc. are written to the log.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of files uploaded to a social networking site.  
*Shadow copies of uploaded files are written to the log.*

## Telegram

Audit and shadowing rights applicable to the Telegram protocol:

- **Audit: Connection** - Enables the auditing of attempts to connect Telegram Desktop to a Telegram server.  
*The Connection action is written to the log.*



- **Audit: Web Connection** - Enables the auditing of attempts to connect to the Telegram Web host. *The Connection action, the IP address with the port number and the name of the host, and the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log. To distinguish the Telegram Web connection from other Telegram connections, Web is indicated in the Name field of the record for this connection.*
- **Audit: Incoming Calls** - Enables the auditing of user attempts to receive calls. *The Incoming Call action and Telegram user IDs of all call participants are written to the log. The user ID of the local participant precedes the user ID of a remote participant.*
- **Audit: Incoming Messages** - Enables the auditing of user attempts to receive instant messages. Can be selected only together with **Audit: Outgoing Messages**. *The Chat action and Telegram user IDs of all IM participants are written to the log. The user ID of the local participant precedes the user ID of a remote participant.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file. *The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Calls** - Enables the auditing of user attempts to make calls. *The Outgoing Call action and Telegram user IDs of all call participants are written to the log. The user ID of the local participant precedes the user ID of a remote participant.*
- **Audit: Outgoing Messages** - Enables the auditing of user attempts to send instant messages. Can be selected only together with **Audit: Incoming Messages**. *The Chat action and Telegram user IDs of all IM participants are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file. *The Outgoing File action and the name of the file are written to the log.*
- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages. *Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Telegram. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files. *Shadow copies of received files are written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages. *Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Telegram. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files. *Shadow copies of sent files are written to the log.*

## Telnet

Audit and shadowing rights applicable to the Telnet protocol:

- **Audit: Connection** - Enables the auditing of user attempts to connect to a Telnet site. *The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*

## Torrent

Audit and shadowing rights applicable to the Torrent protocol:

- **Audit: Connection** - Enables the auditing of the initial user attempt to connect to a remote host over the protocol.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*

## Viber

Audit and shadowing rights applicable to the Viber protocol:

- **Audit: Connection** - Enables the auditing of user attempts to sign in to a Viber account.  
*The Connection action is written to the log.*
- **Audit: Incoming Calls** - Enables the auditing of user attempts to receive calls.  
*The Incoming Call action and Viber user IDs of all call participants are written to the log. The user ID of the local participant precedes the user ID of a remote participant.*
- **Audit: Incoming Messages** - Enables the auditing of user attempts to receive instant messages.  
*The Chat action and Viber user IDs of all IM participants are written to the log. The user ID of the local participant precedes the user ID of a remote participant.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file.  
*The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Calls** - Enables the auditing of user attempts to make calls.  
*The Outgoing Call action and Viber user IDs of all call participants are written to the log. The user ID of the local participant precedes the user ID of a remote participant.*
- **Audit: Outgoing Messages** - Enables the auditing of user attempts to send instant messages.  
*The Chat action and Viber user IDs of all IM participants are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file.  
*The Outgoing File action and the name of the file are written to the log.*
- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages.  
*Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Viber. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files.  
*Shadow copies of received files are written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages.  
*Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Viber. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files.  
*Shadow copies of sent files are written to the log.*

## Web Mail

Audit and shadowing rights applicable to the Web Mail protocol:

- **Audit: Connection** - Enables the auditing of user attempts to access Webmail.  
*The Connection action, the IP address with the port number and the name of the host, the name of the protocol are written to the log. If IP address to host name resolution fails, the host name is not written to the log.*
- **Audit: Outgoing Messages, Outgoing Files** - Enables the auditing of user attempts to send an e-mail message with or without attachments.  
*The Outgoing Message action, the name of the e-mail provider (such as Yahoo, Gmail, Hotmail (Outlook.com), etc.), the number of attachments, the e-mail address of the sender and recipients, the message subject are written to the log. The sender address precedes recipient addresses (sender => recipient1, recipient2).*  
*The number of attachments is always written to the Audit Log.*
- **Shadowing: Outgoing Messages, Outgoing Files** - Enables the shadow copying of sent e-mail messages with or without attachments.  
*Shadow copies of sent e-mail messages with or without attachments are written to the log as .eml files. These files can be opened, for example, in Microsoft Outlook Express, Windows Mail, or Mozilla Thunderbird.*  
*The number of attachments is always written to the Shadow Log.*

---

### Note

Web-mail services automatically save drafts of messages. DeviceLock handles saving a draft as sending a message.

---

## Web Search

Audit and shadowing rights applicable to the Web Search protocol:

- **Audit: Search** - Enables the auditing of user attempts to submit a request on a web search site or enter a URL containing a search request into the web browser's address string.  
*The Search action, the name of the web search service along with the search string entered by the user, the IP address with the port number and the name of the webhost, and the name of the protocol are written to the log.*
- **Shadowing: Search** - Enables the shadow copying of the search request entered by the user.  
*A shadow copy of each search request is written to the log.*

## WhatsApp

Audit and shadowing rights applicable to the WhatsApp protocol:

- **Audit: Connection** - Enables the auditing of WhatsApp Desktop attempts to connect to a WhatsApp server.  
*The Connection action is written to the log.*

- **Audit: Web Connection** - Enables the auditing of attempts to connect to the WhatsApp Web host.  
*The Connection action is written to the log. Unlike WhatsApp Desktop connections, Web is indicated in the Name field of the WhatsApp Web connection record.*
- **Audit: Incoming Messages** - Enables the auditing of user attempts to receive instant messages or audio messages. Can be selected only together with **Audit: Outgoing Messages**.  
*The Chat action and WhatsApp user IDs of all chat participants are written to the log. The user ID of the local participant precedes the user ID of a remote participant.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file.  
*The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Messages** - Enables the auditing of user attempts to send instant messages or audio messages. Can be selected only together with **Audit: Incoming Messages**.  
*The Chat action and WhatsApp user IDs of all chat participants are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file.  
*The Outgoing File action and the name of the file are written to the log.*
- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages.  
*Shadow copies of received messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of WhatsApp. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files.  
*Shadow copies of received files are written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages.  
*Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat window) or if the user signs out of Telegram. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files.  
*Shadow copies of sent files are written to the log.*

## Zoom

Audit and shadowing rights applicable to the Zoom protocol:

- **Audit: Connection** - Enables the auditing of user attempts to sign in to a Zoom account.  
*The Connection action is written to the log.*
- **Audit: Incoming Messages** - Enables the auditing of user attempts to receive an instant message.  
*The Chat action and Zoom account names of all the chat participants are written to the log. The name of the local participant precedes the names of the remote participants.*
- **Audit: Incoming Files** - Enables the auditing of user attempts to receive a file.  
*The Incoming File action and the name of the file are written to the log.*
- **Audit: Outgoing Calls** - Enables the auditing of user attempts to participate in a Zoom meeting.  
*The Outgoing Call action and Zoom account names of all the meeting participants are written to the log. The name of the local participant precedes the names of the remote participants.*

- **Audit: Outgoing Messages** - Enables the auditing of user attempts to send an instant message.  
*The Chat action and Zoom account names of all the chat participants are written to the log.*
- **Audit: Outgoing Files** - Enables the auditing of user attempts to send a file.  
*The Outgoing File action and the name of the file are written to the log.*
- **Shadowing: Incoming Messages** - Enables the shadow copying of received instant messages.  
*Shadow copies of received instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat) or if the user signs out of Zoom. It contains an exact record of all received messages.*
- **Shadowing: Incoming Files** - Enables the shadow copying of received files.  
*Shadow copies of received files are written to the log.*
- **Shadowing: Outgoing Messages** - Enables the shadow copying of sent instant messages.  
*Shadow copies of sent instant messages are written to the log as .txt files. A shadow copy of messages is written to the log after 30 minutes of inactivity (that is, 30 minutes after the last active exchange in the chat) or if the user signs out of Zoom. It contains an exact record of all sent messages.*
- **Shadowing: Outgoing Files** - Enables the shadow copying of sent files.  
*Shadow copies of sent files are written to the log.*

## Default Audit and Shadowing

You can define the default audit and shadowing rules for protocols. The default rules apply to the Users and Everyone groups. The following table lists the rights granted to these groups by default.

Group/ Protocol	Users	Everyone
Career Search	Audit: Connection	Audit: Connection
	Audit: Search	Audit: Search
	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
File Sharing	Audit: Connection	Audit: Connection
	Audit: Incoming Files	Audit: Incoming Files
	Audit: POST Requests	Audit: POST Requests
	Audit: Outgoing Files	Audit: Outgoing Files
FTP	Audit: Connection	Audit: Connection
	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Files	Audit: Outgoing Files
HTTP	Audit: Connection	Audit: Connection
	Audit: Incoming Data	Audit: Incoming Data

IBM Notes	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Data	Audit: Outgoing Data
	Audit: POST Requests	Audit: POST Requests
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Incoming Messages	Audit: Incoming Messages
ICQ Messenger	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Incoming Messages	Audit: Incoming Messages
IRC	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Incoming Messages	Audit: Incoming Messages
Jabber	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Incoming Messages	Audit: Incoming Messages
Mail.ru Agent	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Incoming Messages	Audit: Incoming Messages
MAPI	Audit: Incoming Files	Audit: Incoming Files
	Audit: Incoming Messages	Audit: Incoming Messages
	Audit: Connection	Audit: Connection

Skype	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Incoming Calls	Audit: Incoming Calls
	Audit: Incoming Messages	Audit: Incoming Messages
	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Calls	Audit: Outgoing Calls
	Audit: Outgoing Messages	Audit: Outgoing Messages
SMB	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Incoming Files	Audit: Incoming Files
SMTP	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Outgoing Messages	Audit: Outgoing Messages
Social Networks	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Outgoing Messages	Audit: Outgoing Messages
Telegram	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Web Connection	Audit: Web Connection
	Audit: Incoming Calls	Audit: Incoming Calls
	Audit: Incoming Messages	Audit: Incoming Messages
	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Calls	Audit: Outgoing Calls
	Audit: Outgoing Messages	Audit: Outgoing Messages
Telnet	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
	Audit: Connection	Audit: Connection
Torrent	Audit: Connection	Audit: Connection
Viber	Audit: Connection	Audit: Connection
	Audit: Incoming Calls	Audit: Incoming Calls
	Audit: Incoming Messages	Audit: Incoming Messages

	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Calls	Audit: Outgoing Calls
	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
Web Mail	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Search	Audit: Search
WhatsApp	Audit: Connection	Audit: Connection
	Audit: Web Connection	Audit: Web Connection
	Audit: Incoming Messages	Audit: Incoming Messages
	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection
Zoom	Audit: Incoming Messages	Audit: Incoming Messages
	Audit: Incoming Files	Audit: Incoming Files
	Audit: Outgoing Calls	Audit: Outgoing Calls
	Audit: Outgoing Messages	Audit: Outgoing Messages
	Audit: Outgoing Files	Audit: Outgoing Files
	Audit: Connection	Audit: Connection

## Auditing, Shadowing and Alerts Management Tasks

Managing online (regular) audit, shadowing rules and alerts for protocols involves the following tasks:

- [Defining and editing audit and shadowing rules](#)
- [Enabling alerts](#)
- [Undefining audit and shadowing rules](#)



---

## Note

You can define different online vs. offline audit and shadowing rules for the same user or sets of users. Online audit and shadowing rules (Regular Profile) apply to client computers that are working online. Offline audit and shadowing rules (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define offline audit and shadowing rules for protocols, see [Managing Offline Audit, Shadowing and Alerts for Protocols](#).


---

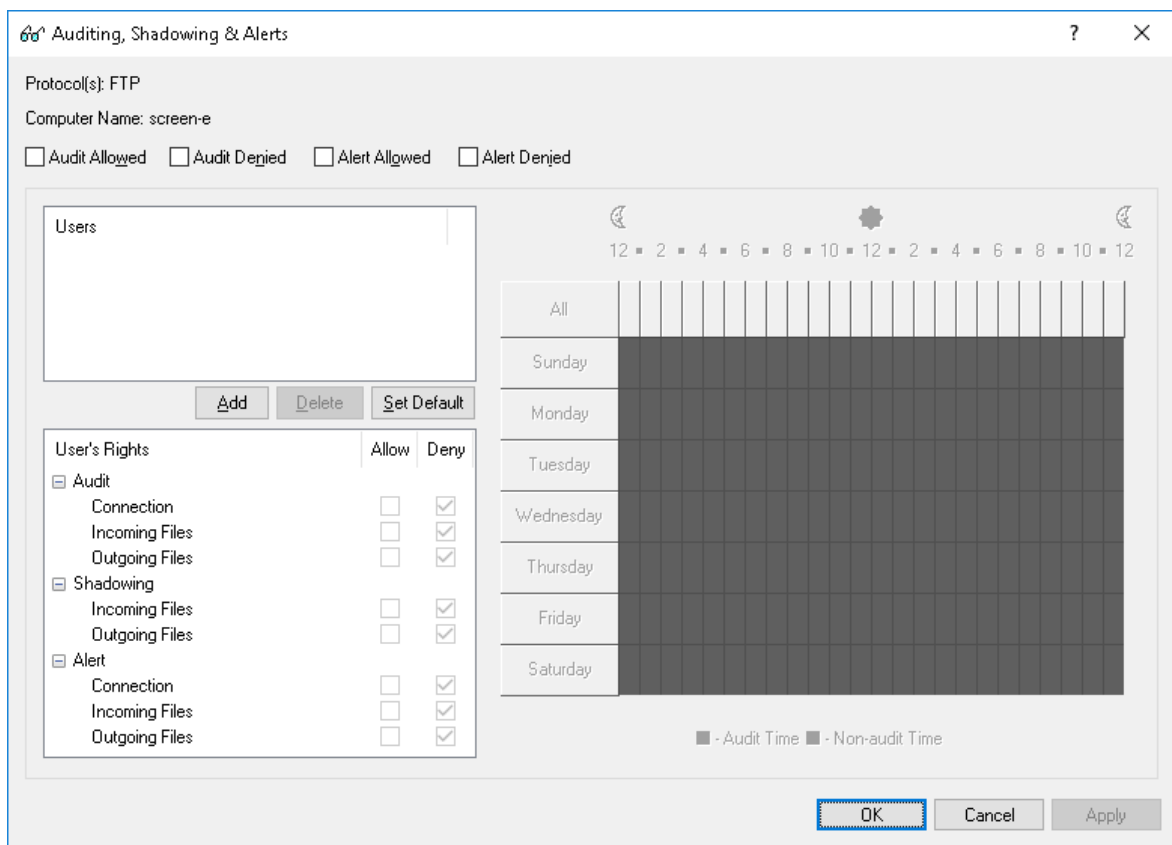
Online audit, shadowing rules and alerts for a protocol can have one of the following states:

- **Not Defined** - Audit, shadowing rules, and alerts are not defined for the protocol.
- **Configured** - Audit, shadowing rules and/or alerts are defined for the protocol.
- **No Audit** - Settings for the protocol do not allow audit, shadowing, and alerts for any accounts.

## Defining and editing audit and shadowing rules

### *To define and edit audit and shadowing rules*

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.  
*When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of on-line rules for each protocol in the Regular column.*
4. In the details pane, do one of the following:
  - Right-click the protocol for which you want to define or edit rules, and then click **Set Auditing, Shadowing & Alerts**.  
- OR -
  - Select the protocol for which you want to define or edit rules, and then click **Set Auditing, Shadowing & Alerts**  on the toolbar.  
- OR -
  - Double-click the protocol for which you want to define or edit rules.*The Auditing, Shadowing & Alerts dialog box appears.*



5. In the **Auditing, Shadowing & Alerts** dialog box, do the following:

**To define the default audit and shadowing rules**

- In the upper-left area of the dialog box, specify which events are written to the Audit Log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a protocol. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a protocol.
- In the upper-left pane of the dialog box, under **Users**, click **Set Default**. The default audit and shadowing rules apply to the Users and Everyone groups. For further details, see [Default Audit and Shadowing](#).

**To define audit and shadowing rules for an additional user or group**

- In the upper-left area of the dialog box, specify which events are written to the audit log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a protocol. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a protocol.
- In the upper-left pane of the dialog box, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
- In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.  
*The users and groups that you added are displayed under Users in the upper-left pane of the Auditing, Shadowing & Alerts dialog box.*
- In the upper-left pane of the **Auditing, Shadowing & Alerts** dialog box, under **Users**, select the user or group.

*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*

- f. In the lower-left pane of the **Auditing, Shadowing & Alerts** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate rights (see [Audit and Shadowing Rights](#)).

*In the right pane of the Auditing, Shadowing & Alerts dialog box, you can specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the rule for the selected user or group will or will not be active. Use the left mouse button to select days and hours when the rule is active (audit time). Use the right mouse button to mark days and hours when the rule is not active (non-audit time).*

#### **To change audit and shadowing rules for an existing user or group**

- a. In the upper-left pane of the dialog box, under **Users**, select the user or group.
- g. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate rights.

#### **To remove an existing user or group and rules**

- In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

*When you remove a user or group, any rules for that user or group will also be removed.*

6. Click **OK** or **Apply**.

## Enabling alerts

You can enable alerts that are sent when a specific user attempts to access a specific protocol.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for specific events, you must configure alert settings in **Service Options** (see [Alerts](#)).

Alerts for specific access-related events are enabled in the **Auditing, Shadowing & Alerts** dialog box. Enabling alerts is similar to defining audit rules (see [Defining and editing audit and shadowing rules](#)), and includes the following basic steps:

- Specify which events will trigger alert notifications. You can enable notification of successful and/or failed attempts to access a protocol. Select the **Alert Allowed** check box to enable notification of successful attempts to access a protocol. Select the **Alert Denied** check box to enable notification of failed attempts to access a protocol.
- Specify users and/or groups whose actions will trigger alert notifications. To do so, in the upper-left pane of the dialog box, under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.
- Specify which user's actions on protocols either will or will not trigger alert notifications. In the upper-left pane of the dialog box, under **Users**, select the user or group that you added. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny an alert right. Alert rights determine which user actions on protocols trigger alert notifications. Alert rights are identical to audit rights. The only difference is that when events

matching specific criteria occur DeviceLock triggers alerts instead of logging these events in the Audit Log. For details on Audit rights for protocols, see [Audit and Shadowing Rights](#).

- Specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on protocols either will or will not trigger alert notifications. To do so, in the right pane of the dialog box, use the left mouse button to select days and hours when the selected user's actions on protocols will trigger alert notifications. Use the right mouse button to mark days and hours when the selected user's actions on protocols will not trigger alert notifications.

---

#### Note

You can enable different online vs. offline protocol-specific alerts. Online alerts (Regular Profile) are generated when client computers are working online. Offline alerts (Offline Profile) are generated when client computers are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to enable offline alerts, see [Managing Offline Audit, Shadowing and Alerts for Protocols](#).

---

## Undefining audit and shadowing rules

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent audit and shadowing rules defined for a particular protocol or protocols from being applied to a specific group of client computers. To do so, you need to return the previously defined rules to the unconfigured state. All undefined DeviceLock Service settings are ignored by client computers.

### **To undefine audit and shadowing rules**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.  
*When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit and shadowing rules.*
4. In the details pane, right-click the protocol whose rules you want to undefine, and then click **Undefine**.  
*You can use the following steps to undefine rules for multiple protocols at a time:*
  - a. In the details pane, click protocols while holding down the SHIFT or CTRL key.
  - b. Right-click the selection, and then click **Undefine**.

# Managing Protocols White List

The Protocols White List lets you selectively allow network communication over any supported protocol regardless of existing protocol blocking settings. The white list is most effective in “least privilege” scenarios when you block all protocol traffic and then specifically authorize only resources required for employees to perform their daily job duties. Resources in the white list can be identified by IPv4 or IPv6 addresses.

For example, suppose that you deny all users access to the SMTP and Web Mail protocols, and then use the white list to let certain users send mail to specific e-mail addresses so that the users can perform their job tasks. By applying these security policies, you can minimize potential risks of data leakage, theft, and misuse.

Under the **Protocols > White List** node in the console tree you can see a list of users and groups that have a protocols white list specified. Protocols in the white list can be specified individually for every user and group.

The shortcut menu of the protocols white list provides the following commands:

- **Delete User** - Deletes the user or group from the white list.
- **Manage** - Opens a dialog box where you can set or change the online (regular) white list.
- **Manage Offline** - Opens a dialog box where you can set or change the offline white list.
- **Load** - Loads a previously saved regular white list from an external file.
- **Load Offline** - Loads a previously saved offline white list from an external file.
- **Save** - Saves the regular white list to an external file.
- **Save Offline** - Saves the offline white list to an external file.
- **Undefine** - Resets the entire regular white list to the unconfigured state. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Undefine Offline** - Resets the entire offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.
- **Remove Offline** - Blocks the inheritance of the offline white list and enforces the regular white list. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).

For further details, see [White List Management Tasks](#).

## White List Rules

When you select a user or group under the **Protocols > White List** node in the console tree, the details pane lists the white list rules specified for that user or group. For each rule, the list provides the following details:

- **Protocol** - The protocol the rule applies to.
- **Name** - The name of the rule.
- **Hosts** - The allowed hosts for this rule.
- **Ports** - The allowed ports for this rule.

- **Send Alert** - Whether sending alerts with this rule is enabled, disabled, or inherited from the protocol level.
- **Log Event** - Whether the audit logging of events associated with this rule is enabled, disabled, or inherited from the protocol level.
- **Shadow Copy** - Whether the shadow copying with this rule is enabled, disabled, or inherited from the protocol level.
- **SSL** - The selected SSL option. Possible values:
  - **Allowed** - Allows SSL connections.
  - **Denied** - Disallows SSL connections.
  - **Required** - Requires that all connections use SSL.
- **Content Inspection** - Whether the content inspection is enabled or not.
- **Extra parameters** - Additional protocol-related parameters:
  - **From** - The allowed sender identifiers for instant messaging and allowed e-mail sender addresses
  - **To** - The allowed recipient identifiers for instant messaging and allowed e-mail recipient addresses
- **Profile** - Possible values:
  - **Regular** - The rule applies to client computers that are working online.
  - **Offline** - The rule applies to computers that are working offline.

You can define different online vs. offline Protocols White Lists for the same user or sets of users. For information about how to define the offline Protocols White List, see [Managing Offline Protocols White List](#).

The shortcut menu on a rule in the details pane provides the following commands:

- **Manage** - Depending on the rule's profile (regular or offline), opens a dialog box that allows you to define the online (regular) or offline Protocols White List.
- **Edit** - Opens a dialog box in which you can view or modify the rule.
- **Send Alert** - Enable or disables alerts for the given rule.
- **Log Event** - Enables or disables the audit logging of events associated with the given rule.
- **Delete** - Deletes the given rule.

For further details, see [White List Management Tasks](#).

## White List Rule Parameters

The white list consists of rules, each associated with a certain protocol. The rule specifies users and groups to which it applies, along with a set of general and protocol-specific parameters.

The general parameters include:

- **Name** - Specifies the name of the rule.
- **Protocol** - Specifies the protocol the rule applies to. The following protocols are supported: Any, Career Search, File Sharing, FTP, HTTP, IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent,

MAPI, Skype, SMB, SMTP, Social Networks, SSL, Telnet, Viber, Web Mail, Web Search, and Zoom. With a white list rule created for the Any protocol, you can allow client connections to the specified hosts and/or ports, regardless of the protocol used to establish connections.

---

**Note**

- Connections allowed by a white list rule created for the Any protocol cannot be blocked by Basic IP Firewall rules.
  - If the Viber protocol is not allowed by the protocol permission settings, white list rules for that protocol have no effect. In this case, Viber users cannot send / receive messages and files.
  - If the HTTP protocol is not allowed by the protocol permission settings, connection to the Zimbra or Outlook Web App (OWA) mail service may fail despite the Web Mail protocol permission. To prevent failures in this case, add the Zimbra and OWA hosts to the white list for the HTTP protocol.
- 

The protocol-specific parameters are as follows:

- [Content Inspection](#)
- [If this rule triggers](#)
- [Hosts](#)
- [Ports](#)
- [File Sharing Services](#)
- [SSL](#)
- [Local sender ID\(s\)](#)
- [Remote recipient ID\(s\)](#)
- [Local sender Email\(s\)](#)
- [Remote recipient Email\(s\)](#)
- [Social Networks](#)
- [Web Mail Services](#)
- [Web Search Services](#)
- [Career Search Services](#)

## Content Inspection

The **Content Inspection** parameter applies to all protocols except Any, SSL, and Telnet.

This parameter specifies whether to enable content inspection for the white-listed connection according to defined Content-Aware Rules (see [Rules for Protocols](#) in [Content-Aware Rules \(Regular Profile\)](#)). If the **Content Inspection** flag is not selected or no Content-Aware Rule is defined for this connection, then content inspection is not performed.

## If this rule triggers

The **If this rule triggers** parameter applies to all protocols.

This parameter specifies the following additional actions to be performed when the rule triggers:

- **Send Alert** - Specifies that an alert is sent whenever the rule triggers.  
DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific white list rule, alert settings must be configured in the service options (see [Alerts](#)).
- **Log Event** - Specifies that an event is logged in the Audit Log whenever the rule triggers.
- **Shadow Copy** - Specifies that a shadow copy of data is created whenever the rule triggers.

When alerts, audit and/or shadowing are enabled or disabled in a white list rule, the rule setting takes precedence over the respective setting for the protocol.

Example: If audit is enabled for a particular protocol and disabled in a rule for that protocol, the triggering of the rule does not cause audit events. If audit is enabled in the rule, then the triggering of the rule causes audit events, even if audit is disabled at the protocol level.

The rule can also inherit the alert, audit and/or shadowing setting from the protocol level. This is the default option, represented by the indeterminate state of the respective check boxes (neither checked nor cleared). The state of each check box can be changed individually.

Example: When a rule inherits the audit setting from the protocol level, the triggering of the rule causes audit events only if audit is enabled for the protocol controlled by that rule.

The Audit Log Viewer displays the following information about any event generated by a white list rule:

- **Type** - Success
- **Date/Time** - The date and time the connection was started, in the following format: dd.mm.yyyy hh:mm:ss. Example: 05.06.2012 14:54:46
- **Source** - The type of the protocol involved.
- **Action** - The user's activity type: either Incoming Connection OR Outgoing Connection
- **Name** - Contains no information.
- **Information** - The IP address with the port number and the fully qualified domain name (FQDN) of the remote host. Example:  
Remote host: 192.168.100.10:99 (mycomputer.mygroup.mydomain.com)
- **Reason** - The cause of the event: White List: "<rule\_name>"
- **User** - The name of the user associated with this event, in the following format: <domain\_name>\<user\_name>.
- **PID** - The identifier of the process associated with this event. Example: 4420
- **Process** - The fully qualified path to the process executable file. Example:  
C:\Program Files\AppFolder\AppName.exe

## Hosts

The **Hosts** parameter applies to the Any, FTP, HTTP, IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, SMB, SMTP, SSL, and Telnet protocols.

This parameter specifies a list of allowed hosts for this rule. If this list is specified, these hosts will not be blocked.



Hosts may be specified in any of the following formats:

- DNS name (for example, `company.com`). You can use the asterisk (\*) wildcard in DNS names (for example, `*.company.com` matches any server name that ends in `.company.com`). For the HTTP protocol, in the **Hosts** field, you can specify not only addresses of websites, but also addresses of individual web pages. In this way, for example, you can white-list only pages at `company.com/section/page`.

---

### Important

Since DeviceLock uses the Hosts local file for host name resolution, an attacker with local administrator rights can tamper with the Hosts file in order to bypass DeviceLock security policies. For example, if the white list allows HTTP access to `company.com`, the attacker can gain access to unauthorized `www.ru` by adding the `194.87.0.50 company.com` entry to the Hosts file. To minimize security risks, we recommend that you secure the Hosts file by selecting the **Prevent Changes In System Configuration Files** check box in the [DeviceLock Administrators](#) parameter setting in [Service Options](#).

---

- IPv4 address (for example, `12.13.14.15`). You can specify a range of IPv4 addresses separated by a dash (-) (for example, `12.13.14.18-12.13.14.28`). You can also specify the subnet mask for the IPv4 address using the following format: `<IPv4 address>/<subnet mask width in bits>` (for example, `3.4.5.6/16`).
- IPv6 address, such as `fe80:0000:0000:0a2f:7e00:0004:533a`, `fe80:0:0:0:a2f:7e00:4:533a`, or `fe80::a2f:7e00:4:533a`.

Multiple hosts must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry. You can specify multiple hosts in different formats described above (for example, `www.microsoft.com; 12.13.14.15, 12.13.14.18-12.13.14.28`).

When adding hosts to the white list, consider the following:

- If objects (images, scripts, video, Flash files, ActiveX, etc.) on a web page are downloaded from other hosts, you must add those hosts to the white list to load the web page correctly.
- If you specify hosts and do not specify ports, the hosts can be accessed through all available ports.
- An application with an embedded SSL certificate (for example, Dropbox, Yandex.Disk, Google Drive, iTunes Google contacts synchronization module, etc.) will fail to connect to its server when the NetworkLock module is active. The NetworkLock module becomes active when you define settings for protocols. To solve this issue, add the server host to the white list for SSL. You can use TcpView to look up the server host. Whitelisting a server host causes all SSL traffic between an application and the specified server host to bypass access control, audit, shadow copying and content filtering.
- When Outlook starts it connects to both the Exchange server and domain controller. If you set the No Access permission for the MAPI protocol and then add a MAPI white list rule, you must specify the host name of your Exchange server and the host name of the domain controller to avoid connection problems.

The same applies to the IBM Notes client, IBM Domino server and to the names of the domain controllers.

## Ports

The **Ports** parameter applies to the Any, FTP, HTTP, ICQ Messenger, IRC, Jabber, Mail.ru Agent, SMTP, SSL, and Telnet protocols.

This parameter specifies the port or ports to open for this rule. If this list is specified, these ports will not be blocked.

You can specify either a single port or an inclusive range of ports separated by a dash (-). For example, to open port 25, specify 25. To open ports 5000 to 5020 inclusive, specify 5000-5020. Multiple ports or port ranges must be separated by a comma (,) or semicolon (;). Example: 25, 36; 8080, 5000-5020. You can also press ENTER after each entry.

---

### Note

If you specify ports and do not specify hosts, users can access all hosts available through the specified ports.

---

## File Sharing Services

The **File Sharing Services** parameter applies to the File Sharing protocol.

This parameter specifies a list of allowed Web-based file storage, sharing and synchronization services for this rule. If this list is specified, information exchanged via these services will not be blocked. For a list of supported storage, sharing and synchronization services, see the [File Sharing protocol description](#).

## SSL

The **SSL** parameter applies to the File Sharing, FTP, HTTP, ICQ Messenger, IRC, SMTP, and Web Mail protocols.

This parameter sets the SSL connection requirements. The following options are available:

- **Allowed** - Allows SSL connections.
- **Denied** - Disallows SSL connections.
- **Required** - Requires that all connections use SSL.

## Local sender ID(s)

The **Local sender ID(s)** parameter applies to the ICQ Messenger, Jabber, Mail.ru Agent, Skype, Viber, and Zoom protocols.

This parameter lists the identifiers of the users who are allowed to send messages and files, and to make outgoing calls. If this parameter is set, DeviceLock will not block outgoing messages, files and calls from the specified users.

Multiple user identifiers must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry in the list.

In this field, you can use an asterisk (\*) as a substitute for zero or more characters. You can also specify solely an asterisk (\*) to mean “any senders.” It is also possible to use a question mark (?) as a substitute for any single character.

ICQ Messenger users are identified by UIN numbers (for example, 111222). Jabber users are identified by Jabber IDs in the format <user>@<domain>. Mail.ru Agent users are identified by mail.ru e-mail addresses in the format <user>@mail.ru. Skype users are identified by Skype user names. Viber users are identified by Viber user IDs (such as 12345550809). Zoom users are identified by Zoom user IDs (for example, 1236567390 or john@host.net).

## Remote recipient ID(s)

The **Remote recipient ID(s)** parameter applies to the ICQ Messenger, Jabber, Mail.ru Agent, Skype, Viber, and Zoom protocols.

This parameter lists the identifiers of the users who are allowed to receive messages, files and calls. If this parameter is set, DeviceLock will not block outgoing messages, files and calls to the specified users.

Multiple user identifiers must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry in the list.

In this field, you can use an asterisk (\*) as a substitute for zero or more characters. You can also specify solely an asterisk (\*) to mean “any recipients.” It is also possible to use a question mark (?) as a substitute for any single character.

ICQ Messenger users are identified by UIN numbers (for example, 111222). Jabber users are identified by Jabber IDs in the format <user>@<domain>. Mail.ru Agent users are identified by mail.ru e-mail addresses in the format <user>@mail.ru. Skype users are identified by Skype user names. Viber users are identified by Viber user IDs (such as 12345550809). Zoom users are identified by Zoom user IDs (for example, 1236567390 or john@host.net).

## Local sender Email(s)

The **Local sender Email(s)** parameter applies to the IBM Notes, MAPI, SMTP and Web Mail protocols.

This parameter specifies a list of allowed e-mail senders for this rule. If this list is specified, mail from these senders will not be blocked. Use the following format for a sender address:  
<user>@<domain> (or <user>/<domain> for IBM Notes).

Multiple e-mail addresses must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry in the list.

In this field, you can use an asterisk (\*) as a substitute for zero or more characters. You can also specify solely an asterisk before or after the “at” sign (@) in an e-mail address. For example, to allow

mail delivery from all users in a certain domain, type \*@domain (or \*/domain for IBM Notes). It is also possible to use a question mark (?) as a substitute for any single character.

---

#### Note

When adding senders/recipients to the white list for Web Mail, consider the following: Messages sent from a Web mail application are kept in the **Sent Items** folder and can be forwarded to any address from any computer.

---

## Remote recipient Email(s)

The **Remote recipient Email(s)** parameter applies to the IBM Notes, MAPI, SMTP and Web Mail protocols.

This parameter specifies a list of allowed e-mail recipients for this rule. If this list is specified, mail to these recipients will not be blocked. Use the following format for a recipient address:

<user>@<domain> (or <user>/<domain> for IBM Notes).

Multiple e-mail addresses must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry in the list.

In this field, you can use an asterisk (\*) as a substitute for zero or more characters. You can also specify solely an asterisk before or after the “at” sign (@) in an e-mail address. For example, to allow mail delivery to all users in a certain domain, type \*@domain (or \*/domain for IBM Notes). It is also possible to use a question mark (?) as a substitute for any single character.

## Social Networks

The **Social Networks** parameter applies to the Social Networks protocol.

This parameter specifies a list of allowed social networking sites for this rule. If this list is specified, these social networking sites will not be blocked. For a list of supported social networking sites, see the [Social Networks protocol description](#).

## Web Mail Services

The **Web Mail Services** parameter applies to the Web Mail protocol.

This parameter specifies a list of allowed Web-based e-mail services for this rule. If this list is specified, e-mail messages sent through these mail services will not be blocked. For a list of supported Web-based e-mail services, see the [Web Mail protocol description](#).

## Web Search Services

The **Web Search Services** parameter applies to the Web Search protocol.

This parameter specifies a list of allowed web-search service providers for this rule. If the list is specified, the DeviceLock Service does not block search requests issued to the providers selected in this list. For a list of supported providers, see the [Web Search protocol description](#).

## Career Search Services

The **Career Search Services** parameter applies to the Career Search protocol.

This parameter specifies a list of allowed web-based job search providers for this rule. If the list is specified, the DeviceLock Service does not block requests issued to the providers selected in this list. For a list of supported providers, see the [Career Search protocol description](#).

## White List Management Tasks

Managing the online (regular) Protocols White List involves the following tasks:

- [Defining Protocols White List](#)
- [Editing Protocols White List](#)
- [Copying rules of Protocols White List](#)
- [Exporting and importing Protocols White List](#)
- [Undefining Protocols White List](#)
- [Deleting rules of Protocols White List](#)

---

### Note


You can define different online vs. offline Protocols White Lists for the same user or sets of users. The online Protocols White List (Regular Profile) applies to client computers that are working online. The offline Protocols White List (Offline Profile) applies to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define the offline Protocols White List, see [Managing Offline Protocols White List](#).

---

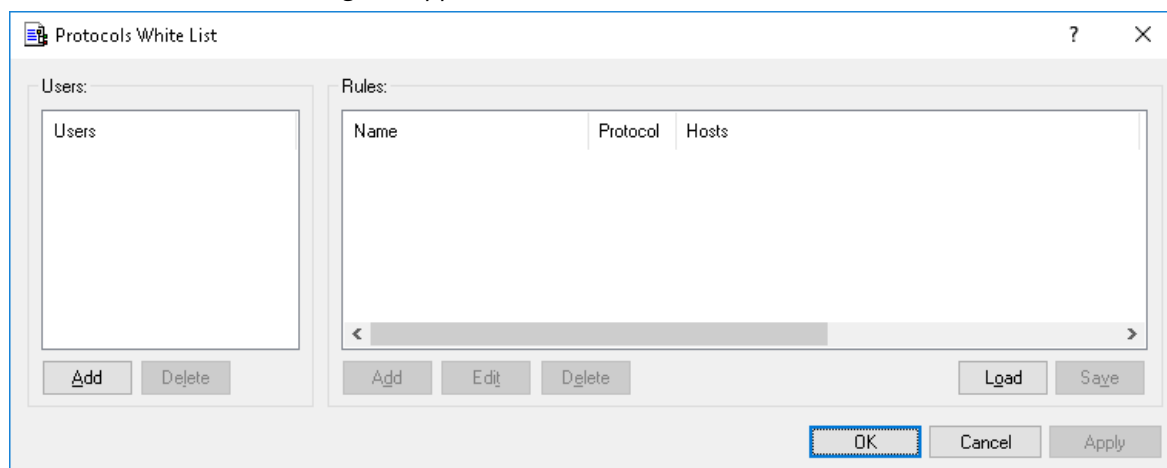
## Defining Protocols White List

### *To define the Protocols White List*

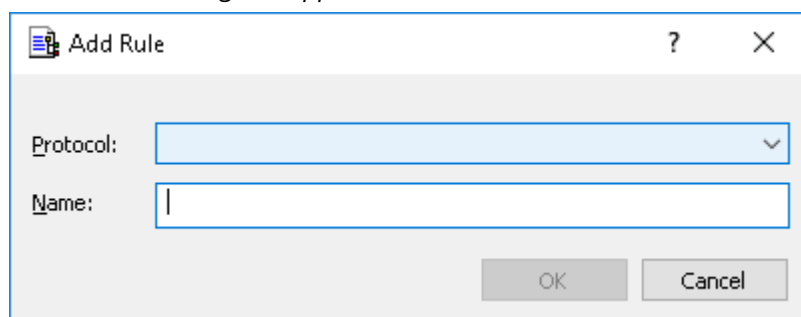
1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.

3. Under **Protocols**, do one of the following:
  - Right-click **White List**, and then click **Manage**.
  - OR -
  - Select **White List**, and then click **Manage**  on the toolbar.

*The Protocols White List dialog box appears.*



4. In the left pane of the **Protocols White List** dialog box, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the Protocols White List, and then click **OK**.  
*The users and groups that you added are displayed under Users in the left pane of the Protocols White List dialog box.*  
To delete a user or group, in the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group, and then click **Delete**.
6. In the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
7. In the right pane of the **Protocols White List** dialog box, under **Rules**, click **Add**.  
*The Add Rule dialog box appears.*



8. In the **Add Rule** dialog box, specify general and protocol-specific parameters for this rule. To specify general parameters, do the following:
  - To specify the protocol, in the **Protocol** list, click the protocol of your choice.
  - To specify the rule name, in the **Name** box, type a name.

To specify protocol-specific parameters, do the following:

- To enable content inspection, click **Content Inspection**. For more information, see the [Content Inspection](#) parameter description.
- To specify additional actions to be performed when this rule triggers, click **If this rule triggers**. For more information, see [If this rule triggers](#) parameter description.
- To specify the hosts, in the **Hosts** box, type host names or IP addresses separated by a comma or semicolon. For more information on how to specify hosts, see the [Hosts](#) parameter description.
- To specify the ports, in the **Ports** box, type port numbers separated by a comma or semicolon. For more information on how to specify ports, see the [Ports](#) parameter description.
- To specify the Web-based file storage, sharing and synchronization services, under **File Sharing Services**, select the appropriate check boxes. For more information, see the [File Sharing Services](#) parameter description.
- To configure the SSL options, under **SSL**, click any of the following: **Allowed** (allows SSL connections), **Denied** (disallows SSL connections), or **Required** (requires that all connections use SSL).
- To specify the IM local sender ID(s), in the **Local sender ID(s)** box, type user identifiers separated by a comma or semicolon. For more information on how to specify user identifiers, see the [Local sender ID\(s\)](#) parameter description.
- To specify the IM remote recipient ID(s), in the **Remote recipient ID(s)** box, type user identifiers separated by a comma or semicolon. For more information on how to specify user identifiers, see the [Remote recipient ID\(s\)](#) parameter description.
- To specify the e-mail senders, in the **Local sender Email(s)** box, type sender addresses separated by a comma or semicolon. For more information on how to specify sender addresses, see the [Local sender Email\(s\)](#) parameter description.
- To specify the e-mail recipients, in the **Remote recipient Email(s)** box, type recipient addresses separated by a comma or semicolon. For more information on how to specify recipient addresses, see the [Remote recipient Email\(s\)](#) parameter description.
- To specify the social networking sites, under **Social Networks**, select the appropriate check boxes. For more information, see the [Social Networks](#) parameter description.
- To specify the Web-based e-mail services, under **Web Mail Services**, select the appropriate check boxes. For more information, see the [Web Mail Services](#) parameter description.
- To specify the Web search providers, under **Web Search Services**, select the appropriate check boxes. For more information, see the [Web Search Services](#) parameter description.
- To specify the Web-based job search providers, under **Career Search Services**, select the appropriate check boxes. For more information, see the [Career Search Services](#) parameter description.

9. Click **OK**.

*The rule you created is displayed under Rules in the right pane of the Protocols White List dialog box.*

10. Click **OK** or **Apply**.

*The users or groups to which the white list rule applies are displayed under White List in the console tree.*

When you select a user or group to which a white list rule applies in the console tree, in the details pane you can view detailed information regarding this rule (see [White List Rules](#) for details).

## Editing Protocols White List

You can modify parameter values specified for a white list rule any time you want.

### **To edit a white list rule**


1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, click **Manage**, and then do the following:
  - a. In the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the white list rules applied to them under Rules in the right pane of the dialog box.*
  - b. In the right pane of the **Protocols White List** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.  
- OR -  
Right-click the rule, and then click **Edit**.  
- OR -  
Under **Protocols**, expand **White List**, and then do the following:
    - a. Under **White List**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the white list rules applied to them in the details pane.*
  - c. In the details pane, right-click the rule you want to edit, and then click **Edit**.  
- OR -  
In the details pane, double-click the rule you want to edit.  
*The Edit Rule dialog box appears.*
4. In the **Edit Rule** dialog box, modify the rule parameters as required to meet your needs.
5. Click **OK** to apply the changes.



## Copying rules of Protocols White List

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing rules of the Protocols White List.

### **To copy a white list rule**



1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **White List**, and then click **Manage**.  
- OR -
  - Select **White List**, and then click **Manage**  on the toolbar.
4. In the left pane of the **Protocols White List** dialog box that appears, under **Users**, select the user or group to which the rule that you want to copy is applied.  
*By selecting users or groups, you can view the white list rules applied to them under Rules in the right pane of the dialog box.*
5. In the right pane of the **Protocols White List** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.  
*The rule you cut or copy is automatically copied to the Clipboard. You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.*
6. In the left pane of the **Protocols White List** dialog box, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.  
*The users and groups that you added are displayed under Users in the left pane of the Protocols White List dialog box.*
8. In the left pane of the **Protocols White List** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*

9. In the right pane of the **Protocols White List** dialog box, right-click in the **Rules** pane and then click **Paste**.  
*The copied rule is displayed under Rules in the right pane of the Protocols White List dialog box.*
10. Click **OK** or **Apply** to apply the copied rule.

## Exporting and importing Protocols White List



You can export all your current rules of the Protocols White List to a .pwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

### **To export the Protocols White List**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **White List**, and then click **Save**.  
- OR -
  - Select **White List**, and then click **Save**  on the toolbar.  
- OR -
  - Expand **White List**, right-click any user or group specified in the white list, and then click **Save**.  
- OR -
  - Expand **White List**, select any user or group specified in the white list. In the details pane, right-click the white list rule, and then click **Save**.  
- OR -
  - Expand **White List**, select any user or group specified in the white list, and then click **Save**  on the toolbar.  
- OR -
  - Right-click **White List**, and then click **Manage**. In the right pane of the **Protocols White List** dialog box, under **Rules**, click **Save**.
4. In the **Save As** dialog box that appears, specify the name and location of the .pwl file, and then click **Save**.

*When you export the Protocols White List, it is saved in a file with a .pwl extension.*

### **To import the Protocols White List**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **White List**, and then click **Load**.  
- OR -
  - Select **White List**, and then click **Load**  on the toolbar.  
- OR -
  - Expand **White List**, right-click any user or group specified in the white list, and then click **Load**.  
- OR -
  - Expand **White List**, select any user or group specified in the white list. In the details pane, right-click the white list rule, and then click **Load**.  
- OR -
  - Expand **White List**, select any user or group specified in the white list, and then click **Load**  on the toolbar  
- OR -
  - Right-click **White List**, and then click **Manage**. In the right pane of the **Protocols White List** dialog box, under **Rules**, click **Load**.
4. In the **Open** dialog box that appears, locate and select the file you want to import, and then click **Open**.  
*If the Protocols White List is already defined and you choose to import a new white list, the following message is displayed: "Do you want to overwrite existing records (Yes - Overwrite, No - Append)?" In the message box, click Yes to overwrite the existing white list. Click No to append a new white list to the existing white list.*

## Undefined Protocols White List

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent the Protocols White List from being applied to a specific group of client computers. To do so, you need to return the previously defined white list to the unconfigured state. All undefined DeviceLock Service settings are ignored by client computers.

### **To undefine the Protocols White List**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, and then click **Undefine**.

## Deleting rules of Protocols White List

You can delete individual white list rules when they are no longer required.

### **To delete a white list rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Expand **White List**, right-click the user or group to which the rule is applied, and then click **Delete user**.  
*When you delete a user or group, the rule associated with this user or group is automatically deleted.*  
- OR -
  - Expand **White List**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.  
- OR -
  - Right-click **White List**, and then click **Manage**. In the left pane of the **Protocols White List** dialog box, under **Users**, select the user or group to which the rule is applied. In the right pane of the **Protocols White List** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

# Managing Basic IP Firewall

The IP Firewall provides control over network traffic that is not covered by [recognized protocols](#) or by the Protocols White List, thus increasing security of network communication. It can be configured to track TCP / UDP packets, allowing only authorized traffic. It can also block any connections to specified hosts, regardless of the permissions configured for the protocols.

The IP Firewall uses a set of rules that either allow or block traffic over a network connection. Each rule specifies the criteria that a packet must match and the resulting action, either allow or deny, that is taken when a match is found. When a client computer attempts to connect to another computer, the firewall automatically checks all the incoming and outgoing traffic packets against your pre-configured rule set. At the first match, the firewall either allows or denies the packets.

By using firewall rules, you can allow only specific network connections, based on the direction of the traffic, protocol, remote host address, and destination ports. Hosts can be identified by IPv4 or IPv6 addresses.

There are two basic approaches when configuring the firewall:

- You deny all traffic and create exceptions to explicitly allow a connection through the firewall.
- You block access to specific hosts and/or ports.

Under the **Protocols > Basic IP Firewall** node in the console tree you can see a list of users and groups that have firewall rules specified. Rules can be specified individually for every user or group.

The shortcut menu of the basic IP firewall provides the following commands:

- **Delete User** - Deletes all firewall rules for a given user or group.
- **Manage** - Opens a dialog box where you can set or change the online (regular) firewall rules.
- **Manage Offline** - Opens a dialog box where you can set or change the offline firewall rules.
- **Load** - Loads a previously saved regular firewall rules from an external file.
- **Load Offline** - Loads a previously saved offline firewall rules from an external file.
- **Save** - Saves the regular firewall rules to an external file.
- **Save Offline** - Saves the offline firewall rules to an external file.
- **Undefine** - Resets all the regular firewall rules to the unconfigured state. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Undefine Offline** - Resets all the offline firewall rules to the unconfigured state. If the offline firewall rules are undefined, the regular firewall rules are applied to offline client computers.
- **Remove Offline** - Blocks the inheritance of the offline firewall rules and enforces the regular firewall rules. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).

For further details, see [Firewall Management Tasks](#).

## Firewall Rules

When you select a user or group under the **Protocols > Basic IP Firewall** in the console tree, the details pane lists the firewall rules specified for that user or group. For each rule, the list provides the following details:

- **Name** - The name of the rule.
- **Override Protocols Permissions** - Shows whether this rule is configured to block access to certain hosts (see the [Override Protocols Permissions](#) parameter description for details).
- **Protocol(s)** - The protocol(s) to which the rule applies: **TCP** and/or **UDP**.
- **Type** - The action the firewall takes for all connections that match the rule's criteria. Possible actions: **Allow** (allows the connection) and **Deny** (blocks the connection).
- **Direction** - The direction of traffic to which the rule applies: **Incoming** and/or **Outgoing**.
- **Hosts** - Shows the specified hosts for this rule.
- **Ports** - Shows the specified ports for this rule.
- **Send Alert** - Shows whether alerts are enabled or disabled for this rule.
- **Log Event** - Shows whether the audit logging of events associated with this rule is enabled or disabled.
- **Profile** - Possible values: **Regular** and **Offline**. **Regular** indicates that the rule applies to client computers that are working online. **Offline** indicates that the rule applies to client computers that are working offline.

You can define different online vs. offline firewall rules for the same user or sets of users. For information about how to define offline firewall rules, see [Managing Offline IP Firewall](#).

The shortcut menu on a rule in the details pane provides the following commands:

- **Manage** - Depending on the rule's profile (regular or offline), opens a dialog box that allows you to define the online (regular) or offline firewall rules.
- **Edit** - Opens a dialog box in which you can view or modify the firewall rule.
- **Send Alert** - Enable or disables alerts for the given rule.
- **Log Event** - Enables or disables the audit logging of events associated with the given rule.
- **Delete** - Deletes the given rule.

For further details, see [Firewall Management Tasks](#).

## Firewall Rule Parameters

Firewall rule parameters specify the conditions under which a network connection is allowed or blocked. A rule has the following parameters:

- [Name](#)
- [Override Protocols Permissions](#)
- [Protocol](#)
- [Type](#)

- [Direction](#)
- [If this rule triggers](#)
- [Hosts](#)
- [Ports](#)

## Name

The **Name** parameter specifies a name to identify the rule.

## Override Protocols Permissions

When the **Override Protocols Permissions** check box is selected, the rule blocks access to the hosts specified in the [Hosts](#) parameter. Such a rule denies any connections to those hosts, regardless of the permissions configured for the protocols. As a result, the user cannot access the host even if access is allowed at the protocol level (see [Managing Permissions for Protocols](#)).

Selecting this check box affects the following rule settings:

- **Protocol** - The TCP and UDP protocols selected. The rule reacts to both TCP and UDP connections.
- **Type** - The Deny type selected. The rule serves to deny connections.
- **Direction** - Both directions selected. The rule denies incoming as well as outgoing connections.
- **Port** - Setting unavailable. The rule denies connections on any TCP or UDP port.

---

### Important

When the **Override Protocols Permissions** check box is selected, an asterisk with a dot (\*. ) in the [Hosts](#) parameter matches not only an arbitrary series of characters that ends with a dot, but also the absence of characters (including a dot). Thus, with the host name \*.host.com, the rule would block access to www.host.com as well as to host.com. To block access to host.com only, exactly this name, host.com, must be specified. Access to www.host.com is not blocked in this case.

---

## Protocol

The **Protocol** parameter specifies the protocol over which the packet is being transferred. The available options are: **TCP** and **UDP**.

## Type

The **Type** parameter determines the action to apply to IP traffic that meets the rule conditions. One of the following actions can be selected:

- **Allow** - Pass IP traffic unhindered.
- **Deny** - Block IP traffic immediately after the start of data transfer.

## Direction

The **Direction** parameter specifies the direction of traffic to which the rule applies. The available options are:

- **Incoming** - The rule applies to incoming traffic.
- **Outgoing** - The rule applies to outgoing traffic.

## If this rule triggers

The **If this rule triggers** parameter specifies the following additional actions to be performed when the rule triggers:

- **Send Alert** - Specifies that an alert is sent whenever the rule triggers. DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific firewall rule, you must configure alert settings in **Service Options** (see [Alerts](#)).
- **Log Event** - Specifies that an event is logged in the Audit Log whenever the rule triggers.

The Audit Log Viewer displays the following information about the event:

- **Type** - Success if traffic allowed by the firewall, Failure if traffic denied by the firewall.
- **Date/Time** - The date and time that the event occurred, in the following format: dd.mm.yyyy hh:mm:ss. Example: 05.06.2012 14:54:46. For allowed traffic - the date and time that the connection started. For denied traffic - the date and time that the packet was dropped.
- **Source** - The type of the protocol involved: IP
- **Action** - The user's activity type: either Incoming Connection Or Outgoing Connection
- **Name** - Contains no information.
- **Information** - The IP address with the port number and the fully qualified domain name (FQDN) of the remote host. Example:  
Remote host: 192.168.100.10:99 (mycomputer.mygroup.mydomain.com)
- **Reason** - The cause of the event: IP Firewall: "<rule\_name>"
- **User** - The name of the user associated with this event, in the following format: <domain\_name>\<user\_name>.
- **PID** - The identifier of the process associated with this event. Example: 4420
- **Process** - The fully qualified path to the process executable file. Example:  
C:\Program Files\AppFolder\AppName.exe

## Hosts

The **Hosts** parameter specifies remote hosts (computers, servers, websites, etc.) to which the rule applies.

Hosts can be specified in any of the following formats:



- DNS name or resource URI (for example, `www.host.com` or `www.host.com/path/resource`). An asterisk (\*) can be used to match an arbitrary series of characters in a name or URI (for example, `*.host.com` matches any name that ends with `.host.com`).

---

### Important

When the [Override Protocols Permissions](#) check box is selected, an asterisk with a dot (\*.) in the DNS name or resource URI matches not only an arbitrary series of characters that ends with a dot, but also the absence of characters, including a dot. Thus, with the host name `*.host.com`, such a rule would block access to `www.host.com` as well as to `host.com`. To block access to `host.com` only, exactly this name, `host.com`, must be specified. Access to `www.host.com` is not blocked in this case.

---

- IPv4 address (for example, `12.13.14.15`). You can specify a range of IPv4 addresses separated by a dash (-) (for example, `12.13.14.18-12.13.14.28`).
- IPv6 address, such as `fe80:0000:0000:0a2f:7e00:0004:533a`, `fe80:0:0:a2f:7e00:4:533a`, or `fe80::a2f:7e00:4:533a`.

Multiple hosts must be separated by a comma (,) or semicolon (;). You can also press ENTER after each entry. You can specify multiple hosts in different formats described above (for example, `www.microsoft.com; 12.13.14.15, 12.13.14.18-12.13.14.28`).

---

### Note

If you specify hosts and do not specify ports, the rule will either allow or block all client connections to the specified hosts.

---

## Ports

The **Ports** parameter specifies the ports on remote hosts to which the rule applies. You can specify either a single port or an inclusive range of ports separated by a dash (-). For example, to open port 110, specify 110. To open ports 5000 to 5020 inclusive, specify 5000-5020. Multiple ports or port ranges must be separated by a comma (,) or semicolon (;). For example, 110, 36; 8080, 5000-5020. You can also press ENTER after each entry.

---

### Note

If you specify ports and do not specify hosts, the rule will either allow or block all client connections to the specified ports.

---

## Firewall Management Tasks

Managing online (regular) firewall involves the following tasks:

- [Defining firewall rules](#)
- [Editing firewall rules](#)
- [Copying firewall rules](#)
- [Exporting and importing firewall rules](#)

- [Undefined firewall rules](#)
- [Deleting firewall rules](#)

You can manage firewall rules using DeviceLock Management Console, DeviceLock Group Policy Manager, or DeviceLock Service Settings Editor.

---

**Note**

You can define different online vs. offline rules for the same user or user groups. Online rules (Regular Profile) apply to client computers that are online. Offline rules (Offline Profile) apply to client computers that are offline. By default, DeviceLock employs offline rules when the network cable is unplugged from the client computer. For details on offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For instructions on defining offline rules, see [Managing Offline IP Firewall](#).

---

## Defining firewall rules

When defining firewall rules, consider the following:

- When the Allow and Deny rules are applied in conjunction, all Allow rules override the Deny rules for both incoming and outgoing traffic.
- Protocol permissions take precedence over firewall rules, except for rules with the [Override Protocols Permissions](#) option enabled, which block access regardless of those permissions.

---


**Important**

Rules with the [Override Protocols Permissions](#) option enabled do not block access allowed by Protocols White List rules for the protocols Any and/or SSL. They also do not block access via protocols not [recognized in NetworkLock](#), provided that access is allowed by other firewall rules.

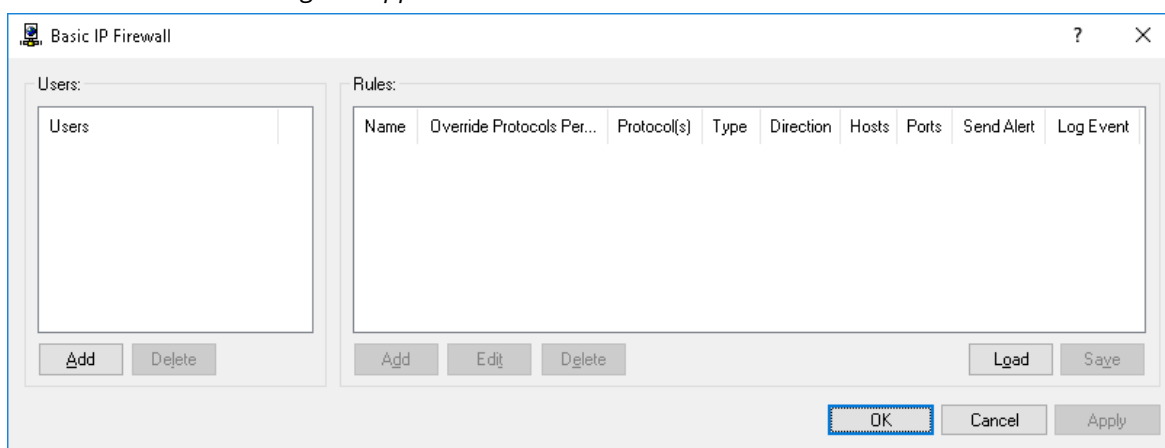
---

- Some applications, for example, Windows built-in applications (such as Remote Desktop) use system processes to transfer data. To block such applications, you must create and apply a firewall rule to the account that is used by the application's data transfer process.
- When users try to establish a connection to which they are denied access, they receive a Basic IP Firewall blocked message, if **Basic IP Firewall blocked message** is enabled in **Service Options**. For details on this message, see the [Basic IP Firewall blocked message](#) parameter description in [Service Options](#).
- The communication between DeviceLock Service and DeviceLock Enterprise Server as well as between DeviceLock Service and DeviceLock Management Console is always allowed, regardless of firewall settings.
- The administrator can enable alerts to be sent upon triggering a particular firewall rule. Alerts are enabled when defining the rule.  
DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a firewall rule, DeviceLock Service alert settings must be configured (see [Alerts](#)).

### ***To define a firewall rule***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Basic IP Firewall**, and then click **Manage**.
  - OR -
  - Select **Basic IP Firewall**, and then click **Manage**  on the toolbar.

*The Basic IP Firewall dialog box appears.*



4. In the left pane of **the Basic IP Firewall** dialog box, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the firewall rule, and then click **OK**.  
*The users and groups that you added are displayed under Users in the left pane of the Basic IP Firewall dialog box.*  
To delete a user or group, in the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group, and then click **Delete**.
6. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
7. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.  
*The Add Rule dialog box appears.*

8. In the **Add Rule** dialog box, specify the firewall rule parameters:
  - To specify the rule name, in the **Name** box, type a name.
  - To block access to the hosts specified by the **Hosts** setting, select the **Override Protocols Permissions** check box. For more information, see the [Override Protocols Permissions](#) parameter description.
  - To specify the protocol, under **Protocol**, select the check box next to the protocol of your choice. For more information, see the [Protocol](#) parameter description.
  - To specify what actions the firewall takes for all connections that match the rule's criteria, under **Type**, click either of the following options: **Allow** or **Deny**. For more information, see the [Type](#) parameter description.
  - To specify the direction of traffic to which the rule applies, under **Direction**, select the appropriate check box. For more information, see the [Direction](#) parameter description.
  - To specify additional actions to be performed when the rule triggers, under **If this rule triggers**, select the appropriate check box. For more information, see the [If this rule triggers](#) parameter description.
  - To specify the remote hosts to which the rule applies, in the **Hosts** box, type host names or IP addresses separated by a comma or semicolon. For more information, see the [Hosts](#) parameter description.
  - To specify the ports on remote hosts to which the rule applies, in the **Ports** box, type port numbers separated by a comma or semicolon. For more information, see the [Ports](#) parameter description.
9. Click **OK**.

*The rule you created is displayed under Rules in the right pane of the Basic IP Firewall dialog box.*
10. Click **OK** or **Apply**.

*The users or groups to which the firewall rule applies are displayed under Basic IP Firewall in the console tree.*

When you select a user or group to which a firewall rule applies in the console tree, in the details pane you can view detailed information regarding this rule (see [Firewall Rules](#) for details).

## Editing firewall rules

You can modify parameter values specified for a firewall rule any time you want.

### **To edit a firewall rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.

If using DeviceLock Service Settings Editor, do the following:

    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.

- d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
  - a. Open Group Policy Object Editor.
- e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, click **Manage**, and then do the following:
  - a. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the firewall rules applied to them under Rules in the right pane of the dialog box.*
  - b. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.  
- OR -  
Right-click the rule, and then click **Edit**.  
- OR -  
Under **Protocols**, expand **Basic IP Firewall**, and then do the following:
    - a. Under **Basic IP Firewall**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the firewall rules applied to them in the details pane.*
  - c. In the details pane, right-click the rule you want to edit, and then click **Edit**.  
- OR -  
In the details pane, double-click the rule you want to edit.  
*The Edit Rule dialog box appears.*
4. In the **Edit Rule** dialog box, modify the rule parameters as required to meet your needs.
5. Click **OK** to apply the changes.

## Copying firewall rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing firewall rules.


### To copy a firewall rule

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.

e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.

3. Under **Protocols**, do one of the following:

- Right-click **Basic IP Firewall**, and then click **Manage**.
- OR -
- Select **Basic IP Firewall**, and then click **Manage**  on the toolbar.

*The Basic IP Firewall dialog box appears.*

4. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.

*By selecting users or groups, you can view the firewall rules applied to them under Rules in the right pane of the dialog box.*

5. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

*The rule you cut or copy is automatically copied to the Clipboard. You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.*

You can copy and then paste several rules at a time. Hold down the SHIFT key or the CTRL key while you click each rule, right-click one of them, and then click **Copy**.

6. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.

*The Select Users or Groups dialog box appears.*

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

*The users and groups that you added are displayed under Users in the left pane of the Basic IP Firewall dialog box.*

8. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*

9. In the right pane of the **Basic IP Firewall** dialog box, right-click in the **Rules** pane and then click **Paste**.

*The copied rule is displayed under Rules in the right pane of the Basic IP Firewall dialog box.*

10. Click **OK** or **Apply** to apply the copied rule.



## Exporting and importing firewall rules

You can export all your current firewall rules to a .ipp file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

### To export firewall rules



1. If using DeviceLock Management Console, do the following:

- a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.

- b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Basic IP Firewall**, and then click **Save**.  
- OR -
  - Select **Basic IP Firewall**, and then click **Save**  on the toolbar.  
- OR -
  - Expand **Basic IP Firewall**, right-click any user or group specified in the firewall rule, and then click **Save**.  
- OR -
  - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule. In the details pane, right-click the firewall rule, and then click **Save**.  
- OR -
  - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule, and then click **Save**  on the toolbar.  
- OR -
  - Right-click **Basic IP Firewall**, and then click **Manage**. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Save**.
4. In the **Save As** dialog box that appears, specify the name and location of the .ipp file, and then click **Save**.  
*When you export firewall rules, they are saved in a file with the .ipp file name extension.*

### **To import firewall rules**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Basic IP Firewall**, and then click **Load**.  
- OR -
  - Select **Basic IP Firewall**, and then click **Load**  on the toolbar.  
- OR -
  - Expand **Basic IP Firewall**, right-click any user or group specified in the firewall rule, and then click **Load**.  
- OR -
  - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule. In the details pane, right-click the firewall rule, and then click **Load**.  
- OR -
  - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule, and then click **Load**  on the toolbar.  
- OR -
  - Right-click **Basic IP Firewall**, and then click **Manage**. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Load**.
4. In the **Open** dialog box that appear, locate and select the file you want to import, and then click **Open**.  
*If firewall rules are already defined and you choose to import new firewall rules, the following message is displayed: "Do you want to overwrite existing records (Yes - Overwrite, No - Append)?" In the message box, click Yes to overwrite the existing firewall rules. Click No to append new firewall rules to the existing firewall rules.*

## Undefining firewall rules

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent firewall rules from being applied to a specific group of client computers. To do so, you need to return the previously defined firewall rules to the unconfigured state. All undefined DeviceLock Service settings are ignored by client computers.

### **To undefine firewall rules**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - c. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.



2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Undefine**.

## Deleting firewall rules

You can delete individual firewall rules when they are no longer required.

### **To delete a firewall rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Expand **Basic IP Firewall**, right-click the user or group to which the rule is applied, and then click **Delete user**.  
*When you delete a user or group, the rule associated with this user or group is automatically deleted.*  
- OR -
  - Expand **Basic IP Firewall**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.  
- OR -
  - Right-click **Basic IP Firewall**, and then click **Manage**. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user or group to which the rule is applied. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

## Managing Security Settings for Protocols

You can use the **Protocols > Security Settings** node to define additional security parameters that affect permissions and audit rules for protocols. For description of these parameters, see [Security Settings Description](#) later in this document.

The shortcut menu on the **Security Settings** node provides the following commands:

- **Manage** - Opens a dialog box where you can enable or disable regular (online) security settings collectively.
- **Manage Offline** - Opens a dialog box where you can enable or disable offline security settings collectively.

When you select the **Security Settings** node, a list of settings appears the details pane. To manage a setting, right-click it in the details pane and use commands from the shortcut menu:

- **Enable** - Enables the online (regular) security setting.
- **Disable** - Disables the online (regular) Security Setting.
- **Undefine** - Resets the regular security setting to the unconfigured state. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).
- **Enable Offline** - Enables the offline security setting.
- **Disable Offline** - Disables the offline security setting.
- **Undefine Offline** - Resets all the previously defined offline security settings to the unconfigured state. If offline security settings are undefined, regular security settings are applied to offline client computers.
- **Manage** - Opens a dialog box where you can enable or disable regular (online) security settings collectively.
- **Manage Offline** - Opens a dialog box where you can enable or disable offline security settings collectively.
- **Remove Offline** - Blocks the inheritance of offline security settings and enforces regular security settings. Available only in [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#).

To change online (regular) security setting, you can double-click the setting in the details pane to switch its state (**enable/disable**). Alternatively, you can choose the **Manage** command from the shortcut menu or click the appropriate button on the toolbar.

For further details, see [Security Settings Management Tasks](#).

## Security Settings Description

DeviceLock provides the following security settings for protocols:

- **Block unrecognized outgoing SSL traffic** - If enabled, causes DeviceLock Service to audit and block all unrecognized outgoing SSL traffic. Otherwise, even if the protocols are locked, all unrecognized outgoing SSL traffic is not blocked and audit is not performed for it.
- **Block IP addresses in URL** - If enabled, causes DeviceLock Service to block connections by any URL containing an IP address even if the user is allowed to use a protocol. This setting affects all protocols except the following: FTP, IBM Notes, IRC, Jabber, MAPI, SMB, SMTP, Telnet, and Torrent. By default, it is disabled.

For protocols affected by this setting, access control, auditing, and shadowing for URLs that contain an IP address are performed at the HTTP protocol level. When DeviceLock Service is

configured to deny access via HTTP, it blocks connections by URLs containing an IP address for all those protocols, regardless of the **Block IP addresses in URL** setting.

---

### Important

If the Protocols White List allows Any protocol access to certain IP addresses, the **Block IP addresses in URL** setting will not block connections to those IP addresses.

---

- **Block proxy traffic** - If enabled, causes DeviceLock Service to audit and block all traffic that flows through a proxy server. The following proxy servers are supported: HTTP, SOCKS4, and SOCKS5.
- **Block network if BFE service is stopped (Windows 8 and later)** - If enabled, causes DeviceLock Service to block all network traffic when the Base Filtering Engine (BFE) system service is stopped. If this setting is disabled and the Base Filtering Engine service is stopped, NetworkLock is unable to control the network traffic on Windows 8 and later systems. To enable this setting, the NetworkLock policy (any protocol-related DeviceLock Service permissions or rules) must be defined. Otherwise, this setting has no effect.
- **Intercept MS Lync connections** - If enabled, causes DeviceLock Service to intercept network traffic from Microsoft Lync 2010 or Microsoft Office Communicator. To enable this setting, the NetworkLock policy (any protocol-related DeviceLock Service permissions or rules) must be defined. Otherwise, this setting has no effect.
- **Block Tor Browser traffic** - If enabled, causes DeviceLock Service to block connection to the Tor network, preventing the use of the Tor Browser. To enable this setting, the NetworkLock policy (any protocol-related DeviceLock Service permissions or rules) must be defined. Otherwise, this setting has no effect.  
When this setting is in effect, attempts to use the Tor Browser are registered in the Audit Log as connection failure events with Tor Browser specified as the source, and accounted for as denied access requests via the Other protocol in Audit Log reports.
- **Intercept draft MAPI messages** - If enabled, causes DeviceLock Service to control draft folder messages that Outlook saves to the Exchange Server. With this setting enabled, all DeviceLock rules and permissions specified for the MAPI protocol are applied to such drafts. Disable this setting if you do not want DeviceLock to control draft messages.
- **Intercept moved MAPI messages** - If enabled, causes DeviceLock Service to control messages being imported to the Exchange Server from e-mail message export files (.msg files) or other (external) mailboxes. With this setting enabled, all DeviceLock rules and permissions specified for the MAPI protocol are applied to e-mail messages from .msg files or external mailboxes that Outlook sends to the Exchange Server. Disable this setting if you do not want DeviceLock to control such messages.

## Security Settings Management Tasks

Managing online (regular) Security Settings for protocols involves the following tasks:

- [Defining and changing Security Settings](#)
- [Undefining Security Settings](#)

---

## Note

You can define different online vs. offline Security Settings for the same user or sets of users. Online Security Settings (Regular Profile) apply to client computers that are working online. Offline Security Settings (Offline Profile) apply to client computers that are working offline. By default, DeviceLock works in offline mode when the network cable is not connected to the client computer. For detailed information on DeviceLock offline policies, see [DeviceLock Security Policies \(Offline Profile\)](#). For information about how to define offline Security Settings, see [Managing Offline Security Settings for Protocols](#).


---

Online Security Settings for protocols can have one of the following states:

- **Not Configured** - Indicates that Security Settings are not defined for protocols.
- **Enabled** - Indicates that Security Settings are enabled for protocols.
- **Disabled** - Indicates that Security Settings are disabled for protocols.

## Defining and changing Security Settings

### *To define and change Security Settings*

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Select **Security Settings**. In the details pane, right-click the Security Setting, and then click **Enable** or **Disable**.  
*When you select Security Settings in the console tree, they are displayed in the details pane.*  
- OR -
  - Right-click **Security Settings**, and then click **Manage**. In the **Security Settings** dialog box that opens, select or clear the appropriate check box, and then click **OK**.  
*To open the Security Settings dialog box, you can also select Security Settings, and then click Manage  on the toolbar.*

## Undefining Security Settings

If you deploy DeviceLock policies using DeviceLock Group Policy Manager or DeviceLock Service Settings Editor, in some situations you may want to prevent Security Settings defined for protocols

from being applied to a specific group of client computers. To do so, you need to return the previously defined Security Settings to the unconfigured state. All undefined DeviceLock Service settings are ignored by client computers.

### **To undefine Security Settings**

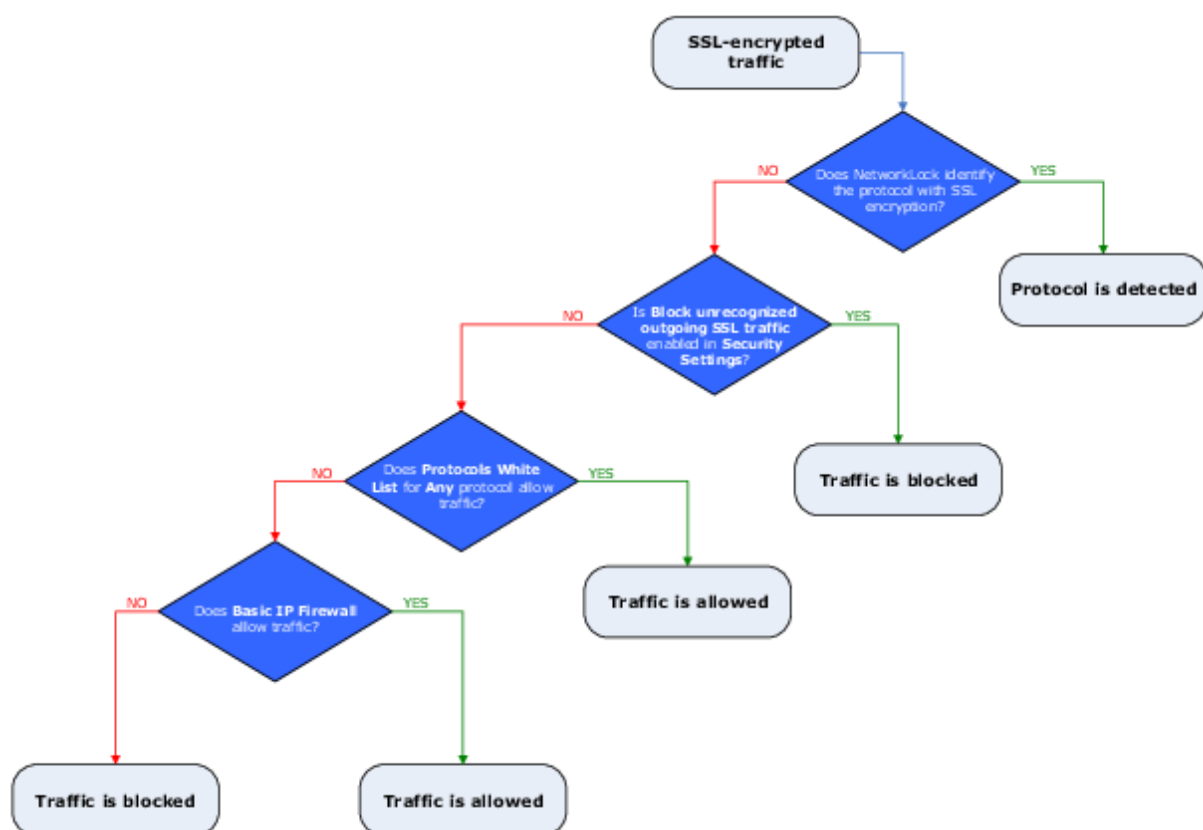
1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Security Settings**.  
*When you select Security Settings in the console tree, they are displayed in the details pane.*
4. In the details pane, right-click the Security Setting you want to undefine, and then click **Undefine**.

## Inspection and Control of SSL-encrypted Traffic

Inspection and control of SSL-encrypted traffic includes a number of sequential steps that can be summarized as follows:

1. Identify the protocol used with SSL. When the protocol is identified, DeviceLock checks whether the user is allowed to connect via that protocol (see [diagram](#) in the [Managed Access Control](#) section earlier in this document).
2. Check whether the [Block unrecognized outgoing SSL traffic](#) option is enabled (see [Managing Security Settings for Protocols](#)).
3. Check whether traffic is allowed by a white list rule created for the Any protocol (see [Protocol](#) option description in [Managing Protocols White List](#)).
4. Check whether traffic is allowed by a firewall rule.

In the following diagram you can see how DeviceLock inspects SSL-encrypted traffic and applies appropriate security measures based on the policies defined.



# DeviceLock Security Policies (Offline Profile)

## Overview

Today, organizations have many users who must continue working with business-critical information when they are disconnected from the corporate network. For example, traveling sales representatives, insurance agents and regional inspectors increasingly use corporate laptops or notebooks at disconnected locations. Protecting the sensitive information on these mobile computers has become a priority for many organizations.

DeviceLock provides greater protection of sensitive corporate information in disconnected environments. You can control user access to devices and protocols as well as the shadow copying of the data written by the user or transmitted over the network in different offline scenarios. DeviceLock also offers more management flexibility, as you can define different online vs. offline security policies for the same user or set of users.

A user's online policies are applied when connected to the corporate network, or specified DeviceLock Enterprise Servers, or Active Directory domain controllers. Offline policies are applied when the user is working disconnected from the corporate network, or specified DeviceLock Enterprise Servers, or Active Directory domain controllers.

For DeviceLock to enforce different policies in online vs. offline scenarios, configure settings for two profile types:

- **Regular Profile** - These settings are used by client computers that are working online.
- **Offline Profile** - These settings are used by client computers that are working offline (for example, when users travel with their corporate laptops).

If offline profile settings are not configured, regular profile settings are used in both online and offline scenarios.

You can use different regular vs. offline profiles for Permissions, Auditing, Shadowing rules and Alerts, USB Devices White List, Media White List, Protocols White List, Content-Aware Rules, Basic IP Firewall, and Security Settings. You can manage offline profile settings using DeviceLock Management Console, DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.

The following examples describe typical scenarios in which you are likely to set different online vs. offline security policies to better protect your corporate data.

- **Scenario 1.** Suppose you have a Finance group in your organization. As an administrator, you can allow members of this group to write files to Removable, Optical Drive, USB, and Floppy devices when they work online. Their online activity will be audited. Any copied files will be shadow copied; and audit and shadow logs will be sent to DeviceLock Enterprise Server. When offline, members of the Finance group will be denied write access.  
*These security policies let you monitor the activity of the Finance group members in real-time mode. By examining audit and shadow logs on DeviceLock Enterprise Server (often on a daily basis), you can respond promptly and appropriately when a data leakage incident occurs. In this case, a user will not*

*be able to copy sensitive information to a device while offline in an attempt to avoid sending shadow copies to DeviceLock Enterprise Server and thus alerting the Security department of the data theft.*

- **Scenario 2.** Imagine Mary, a sales representative of a large company, who has a notebook computer and frequently works out of the office. She needs to be able to provide her business partners with information files resulting from her work. In this situation, you can allow Mary to write certain files to Removable, Optical Drive, USB, and Floppy devices and enable the shadow copying of these files when she works offline. When online, she will be denied write access to the specified device types.

*These security policies give you greater flexibility in managing users within an organization while providing better corporate data security.*

## Configuring Offline Mode Detection Settings

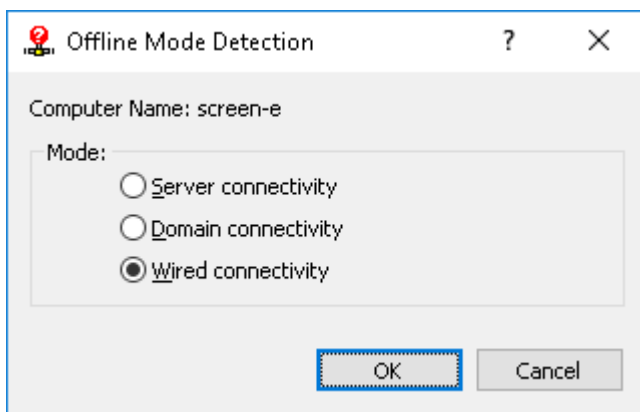
You can define the network characteristics that DeviceLock uses to detect its connection state (whether it is online or offline). By default, DeviceLock works in offline mode when the network cable is not connected to the client computer.

### ***To configure offline mode detection settings***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Select **Service Options**.  
*When you select Service Options in the console tree, they are displayed in the details pane.*
3. In the details pane, do one of the following:
  - Right-click **Offline mode detection**, and then click **Properties**.
  - OR -
  - Double-click **Offline mode detection**.

*The Offline Mode Detection dialog box appears.*





4. In the **Offline Mode Detection** dialog box, click any of the following options:
- **Server connectivity** - The connection state is determined by whether the DeviceLock Service logs can be transferred from the client computer to DeviceLock Enterprise Server. When this option is selected, the computer is considered to work in online mode if the server can receive DeviceLock logs for at least one of the users who are currently using that computer. The server is determined by the [DeviceLock Enterprise Server\(s\)](#) parameter in [Service Options](#).

The computer is considered to work in offline mode if the server cannot receive DeviceLock logs for any one of the users who are currently using that computer. This may occur because the DeviceLock Service is unable to authenticate to any designated DeviceLock Enterprise Server or all designated servers are unavailable.

---

**Note**

DeviceLock certificate-based authentication provides the most reliable way to secure client/server communication. For client/server certificate authentication, the public key must be installed on client computers, while the private key must be installed on DeviceLock Enterprise Server/s.

If the certificate's public key is installed only on client computers, the server will reject connections and client computers will work in offline mode. If the certificate's private key is installed only on DeviceLock Enterprise Server, the server and the client will authenticate each other once a connection is established although this type of authentication is less secure than client/server certificate authentication. For details on DeviceLock certificates, see [DeviceLock Certificates](#).

- **Domain connectivity** - The connection state is determined by whether a connection can be established to a controller of the Active Directory domain to which the client computer belongs. When this option is selected, the computer is considered to work in online mode if it is connected to a controller of its domain. The computer is considered to work in offline mode if it cannot connect to any controller of its domain.  
*With this option, client computers not joined to a domain (workgroup members or stand-alone computers) always work in offline mode.*

- **Wired connectivity** - The connection state is determined by whether the network cable is plugged into the Network Interface Card (NIC) of the client computer. This is the simplest and least secure method of detecting the connection state.


When this option is selected, the computer is considered to work in online mode if the network cable is plugged into its NIC. The computer is considered to work in offline mode if the network cable is unplugged. Please note that only cable connections are taken into account. Wireless network connections (Wi-Fi, etc.) and modem connections are disregarded.

*This option is selected by default.*

5. Click **OK**.

## Switching Between Online and Offline Mode

DeviceLock Service running on client computers automatically detects the connection state and seamlessly switches between online and offline mode every hour and when any of the following events occurs:

- A user boots the computer running DeviceLock Service.  
*DeviceLock Service always starts in offline mode.*
- A user logs on.
- A user right-clicks the DeviceLock Tray Notification Utility icon  in the notification area of the taskbar, and then clicks **Refresh Current State**.  
The DeviceLock Tray Notification Utility icon is displayed in the notification area when [Always show tray icon](#) is enabled in [Service Options](#).
- DeviceLock Service sends audit and shadow logs to DeviceLock Enterprise Server.
- A network interface changes state:
  - A network cable is connected or disconnected.
  - A modem connects or disconnects.
  - A virtual private network (VPN) connection is established or terminated.
  - A wireless network connection using a WiFi card is established or terminated.
  - A DHCP-assigned IP address is used or released.
  - A network card is enabled, disabled, added or removed.
- Changes to DeviceLock Service settings are made.

## Managing Offline Security Policies for Devices

You can manage offline security policies in much the same way as you manage online (regular) policies except for a few variations. This section provides offline profile-specific information as well as basic management procedures. For detailed information on permissions, audit, shadowing rules and alerts, white lists, Security Settings, and Content-Aware Rules, refer to the following sections:

[Permissions \(Regular Profile\)](#)

[Auditing, Shadowing & Alerts \(Regular Profile\)](#)

[USB Devices White List \(Regular Profile\)](#)

[Media White List \(Regular Profile\)](#)

[Security Settings \(Regular Profile\)](#)

[Rules for Devices in Content-Aware Rules \(Regular Profile\)](#)

Managing offline security policies for devices involves the following operations:

- [Managing Offline Permissions for Devices](#)
- [Managing Offline Audit, Shadowing and Alerts for Devices](#)
- [Managing Offline USB Devices White List](#)
- [Managing Offline Media White List](#)
- [Managing Offline Content-Aware Rules for Devices](#)
- [Managing Offline Security Settings for Devices](#)

You can manage offline security policies by using DeviceLock Management Console, Service Settings Editor, or DeviceLock Group Policy Manager.

## Managing Offline Permissions for Devices

For details on the Permissions feature, see [Permissions \(Regular Profile\)](#).

Offline permissions can have one of the following states:


- **Not Configured** - No permission settings are specified for the device type.
- **Configured** - Different accounts are assigned different permissions for the device type.
- **Full Access** - All accounts have full access to the device type.  
This state shows up, for example, when permissions are set only for the “Everyone” account so that it has full access to the device type.
- **No Access** - No accounts have access to the device type.  
This state shows up, for example, when the “Everyone” account is explicitly denied any access to the device type, or permissions are not set for any accounts. Note that the denial for the “Everyone” account overrides all permissions for other accounts.
- **Use Regular** - Inheritance of offline permissions is blocked and regular permissions are enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of regular permissions is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent offline permissions inherited from a higher level from being applied to a specific group of client computers at a lower level.  
For more information on the enforcement of regular permissions, see [Removing offline permissions](#).

Managing offline permissions involves the following tasks:

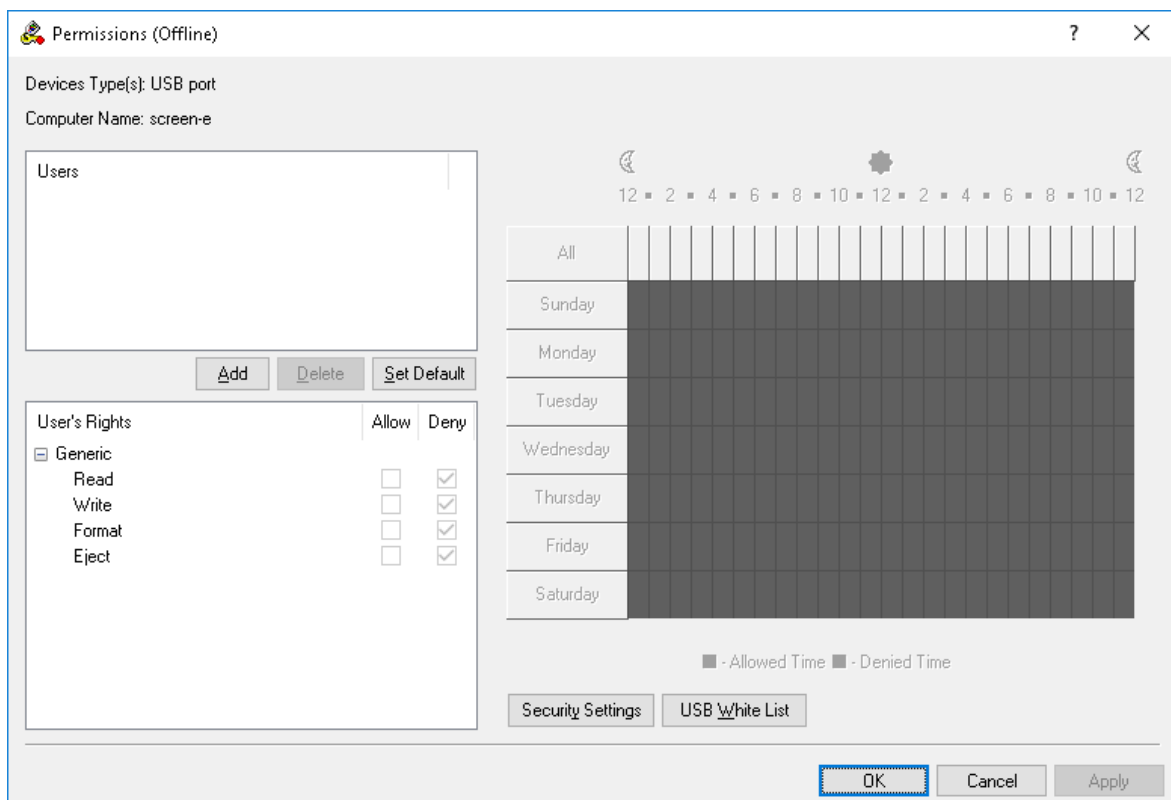
- [Setting and editing offline permissions](#)
- [Undefined offline permissions](#)
- [Removing offline permissions](#)

## Setting and editing offline permissions

### ***To set and edit offline permissions***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Permissions**.  
*When you select Permissions in the console tree, in the details pane you can view device types for which you can set permissions. In the details pane, you can also view the current state of offline permissions for each device type in the Offline column.*
4. In the details pane, do one of the following:
  - Right-click the device type for which you want to set or edit permissions, and then click **Set Offline Permissions**.  
- OR -
  - Select the device type for which you want to set or edit permissions, and then click **Set Offline Permissions**  on the toolbar.

*The Permissions (Offline) dialog box appears.*



5. In the **Permissions (Offline)** dialog box, do the following:

**To set the default permissions**

- In the upper-left pane of the dialog box, under **Users**, click **Set Default**.  
The default permissions are assigned to the Administrators, Everyone, and SYSTEM accounts. For information about which permissions are set for these accounts by default, see [Permissions \(Regular Profile\)](#).

**To set permissions for an additional user or group**

- In the upper-left pane of the dialog box, under **Users**, click **Add**.
- In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.  
*The users and groups that you added are displayed under Users in the upper-left pane of the Permissions (Offline) dialog box.*
- In the upper-left pane of the **Permissions (Offline)** dialog box, under **Users**, select the user or group.  
*You can select multiple users and/ or groups by holding down the SHIFT key or the CTRL key while clicking them.*
- In the lower-left pane of the **Permissions (Offline)** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights.  
*In the right pane of the Permissions (Offline) dialog box, you can set day and time restrictions that narrow user access to devices. Use the left mouse button to select days and hours when the selected user or group will have access to devices. Use the right mouse button to mark days and hours when the selected user or group will not have access to devices.*

**To change permissions for an existing user or group**

- a. In the upper-left pane of the dialog box, under **Users**, select the user or group.
  - e. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights.
- To remove an existing user or group and permissions**
  - In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.
6. Click **OK** or **Apply**.

## Undefining offline permissions

You can reset previously set offline permissions to the unconfigured state. If offline permissions are undefined, regular permissions are applied to offline client computers.

### **To undefine offline permissions**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Permissions**.  
*When you select Permissions in the console tree, in the details pane you can view device types for which you can set permissions. In the details pane you can also view the current state of offline permissions for each device type in the Offline column.*
4. In the details pane, right-click the device type for which you want to undefine offline permissions, and then click **Undefine Offline**.  
*You can undefine offline permissions set for several device types at the same time. To do this, do the following:*
  - a. In the details pane, select several device types by holding down the SHIFT key or the CTRL key while clicking them.
  - b. Right-click the selection, and then click **Undefine Offline**.  
*The offline state of the permissions changes to "Not Configured."*

## Removing offline permissions

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline permissions

and enforce regular permissions on specific lower-level groups of client computers. To enforce regular permissions, offline permissions must be removed.

### **To remove offline permissions**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Permissions**.  
*When you select Permissions in the console tree, in the details pane you can view device types for which you can set permissions. In the details pane you can also view the current state of offline permissions for each device type in the Offline column.*
4. In the details pane, right-click the device type for which you want to remove offline permissions, and then click **Remove Offline**.  
*You can remove offline permissions set for several device types at the same time. To do this, do the following:*
  - a. In the details pane, select several device types by holding down the SHIFT key or the CTRL key while clicking them.
  - b. Right-click the selection and then click **Remove Offline**.  
*The offline state of the permissions changes to "Use Regular."*  
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline Audit, Shadowing and Alerts for Devices

For details on the Auditing & Shadowing feature, see [Auditing, Shadowing & Alerts \(Regular Profile\)](#). For details on the Alerts feature, see [Alerts](#). For information about how to enable online (regular) alerts, see [Auditing, Shadowing & Alerts \(Regular Profile\)](#). For information about how to enable offline alerts, see [Enabling offline alerts](#).

Offline audit, shadowing rules and alerts can have one of the following states:

- **Not Configured** - Offline audit, shadowing rules, and alerts are not defined for the device type.
- **Configured** - Offline audit, shadowing rules and/or alerts are defined for the device type.
- **No Audit** - Offline settings for the device type do not allow audit, shadowing, and alerts for any accounts.
- **Use Regular** - Inheritance of offline audit and shadowing rules is blocked and regular audit and shadowing rules are enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of regular rules is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of

enforcement can be used to prevent offline rules inherited from a higher level from being applied to a specific group of client computers at a lower level.


For more information on the enforcement of regular rules, see [Removing offline audit and shadowing rules](#).

Managing offline audit, shadowing rules and alerts involves the following tasks:

- [Defining and editing offline audit and shadowing rules](#)
- [Enabling offline alerts](#)
- [Undefined offline audit and shadowing rules](#)
- [Removing offline audit and shadowing rules](#)

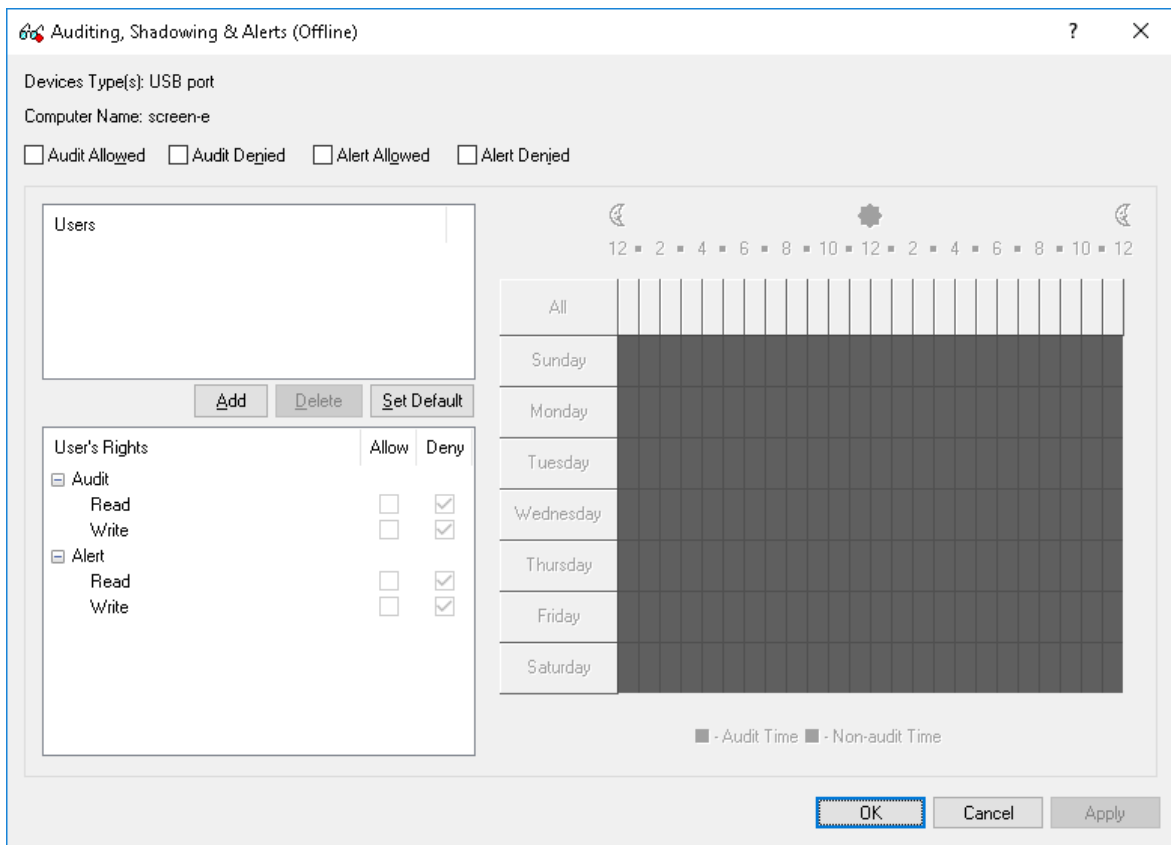
## Defining and editing offline audit and shadowing rules

### ***To define and edit offline audit and shadowing rules***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Auditing, Shadowing & Alerts**.  
*When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view device types for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each device type in the Offline column.*
4. In the details pane, do one of the following:
  - Right-click the device type for which you want to define or edit rules, and then click **Set Offline Auditing, Shadowing & Alerts**.  
- OR -
  - Select the device type for which you want to define or edit rules, and then click **Set Offline Auditing, Shadowing & Alerts**  on the toolbar.

*The Auditing, Shadowing & Alerts (Offline) dialog box appears.*





5. In the **Auditing, Shadowing & Alerts (Offline)** dialog box, do the following:

**To define the default audit and shadowing rules**

- In the upper-left area of the dialog box, specify which events are written to the audit log.  
Select the **Audit Allowed** check box to audit successful attempts to gain access to a device.  
Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a device.
- In the upper-left pane of the dialog box, under **Users**, click **Set Default**.  
The default audit, shadowing rules and alerts apply to members of the Users group and Everyone account. For information about which Audit and Shadowing rights are set for these accounts by default, see [Auditing, Shadowing & Alerts \(Regular Profile\)](#).

**To define audit and shadowing rules for an additional user or group**

- In the upper-left area of the dialog box, specify which events are written to the audit log.  
Select the **Audit Allowed** check box to audit successful attempts to gain access to a device. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a device.
- In the upper-left pane of the dialog box, under **Users**, click **Add**.
- In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.  
*The users and groups that you added are displayed under Users in the upper-left pane of the Auditing, Shadowing & Alerts (Offline) dialog box.*
- In the upper-left pane of the **Auditing, Shadowing & Alerts (Offline)** dialog box, under **Users**, select the user or group.

*You can select multiple users and/ or groups by holding down the SHIFT key or the CTRL key while clicking them.*

- f. In the lower-left pane of the **Auditing, Shadowing & Alerts (Offline)** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate audit and shadowing rights.

*Audit and Shadowing rights determine which user actions on devices are logged to the audit and/or shadow log.*

*In the right pane of the Auditing, Shadowing & Alerts (Offline) dialog box, you can specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on devices will be logged to either the audit or shadow log. Use the left mouse button to select days and hours when the selected user's actions on devices will be logged. Use the right mouse button to mark days and hours when the selected user's actions on devices will not be logged.*

#### **To change audit and shadowing rules for an existing user or group**

- a. In the upper-left pane of the dialog box, under **Users**, select the user or group.
- g. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate audit and shadowing rights.

#### **To remove an existing user or group and rules**

- In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.  
*When you remove a user or group, any rules for that user or group will also be removed.*

6. Click **OK** or **Apply**.

## Enabling offline alerts

Offline alerts for specific access-related events are enabled in the **Auditing, Shadowing & Alerts (Offline)** dialog box. Enabling offline alerts is similar to defining offline audit rules (see [Defining and editing offline audit and shadowing rules](#)) and includes the following basic steps:

- Specify which events will trigger alert notifications. You can enable notification of successful and/ or failed attempts to access a device. Select the **Alert Allowed** check box to enable notification of successful attempts to access a device. Select the **Alert Denied** check box to enable notification of failed attempts to access a device.
- Specify users and/or groups whose actions will trigger alert notifications. To do so, in the upper-left pane of the dialog box, under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.
- Specify which user's actions on devices either will or will not trigger alert notifications. In the upper-left pane of the dialog box, under **Users**, select the user or group that you added. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny an alert right. Alert rights determine which user actions on devices trigger alert notifications. Alert rights are identical to audit rights. The only difference is that when events matching specific criteria occur DeviceLock triggers alerts instead of logging these events in the

Audit Log. For detailed information on Audit rights for devices, see [Auditing, Shadowing & Alerts \(Regular Profile\)](#).

- Specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on devices either will or will not trigger alert notifications. To do so, in the right pane of the dialog box, use the left mouse button to select days and hours when the selected user's actions on devices will trigger alert notifications. Use the right mouse button to mark days and hours when the selected user's actions on devices will not trigger alert notifications.

## Undefining offline audit and shadowing rules

You can return previously defined offline audit and shadowing rules to the unconfigured state. If offline rules are undefined, regular rules are applied to offline client computers.

### **To undefine offline audit and shadowing rules**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Auditing, Shadowing & Alerts**.  
*When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view device types for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each device type in the Offline column.*
4. In the details pane, right-click the device type for which you want to undefine offline audit and shadowing rules, and then click **Undefine Offline**.  
*You can undefine audit and shadowing rules defined for several device types at the same time. To do this, do the following:*
  - a. In the details pane, select several device types by holding down the SHIFT key or the CTRL key while clicking them.
  - b. Right-click the selection, and then click **Undefine Offline**.  
*The offline state of the audit and shadowing rules changes to "Not Configured."*

## Removing offline audit and shadowing rules

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline audit and shadowing rules and enforce regular audit and shadowing rules on specific lower-level groups of

client computers. To enforce regular audit and shadowing rules, offline audit and shadowing rules must be removed.

### **To remove offline audit and shadowing rules**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Auditing, Shadowing & Alerts**.  
*When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view device types for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each device type in the Offline column.*
4. In the details pane, right-click the device type for which you want to remove offline audit and shadowing rules, and then click **Remove Offline**.  
*You can remove audit and shadowing rules defined for several device types at the same time. To do this, do the following:*
  - a. In the details pane, select several device types by holding down the SHIFT key or the CTRL key while clicking them.
  - b. Right-click the selection, and then click **Remove Offline**.  
*The offline state of the audit and shadowing rules changes to "Use Regular."*  
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline USB Devices White List

For details on the USB Devices White List feature, see [USB Devices White List \(Regular Profile\)](#).

The offline USB Devices White List can have one of the following states:


- **Not Configured** - The white list is not defined. The following message is displayed: "Offline USB White List is not configured." This is the default state.
- **Configured** - The white list is defined.
- **Use Regular** - The inheritance of the offline white list is blocked and the regular white list is enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of the regular white list is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent the offline white list inherited from a higher level from being applied to a specific group of client computers at a lower level.  
For more information on the enforcement of the regular white list, see [Removing offline USB Devices White List](#).

Managing the offline USB Devices White List involves the following tasks:

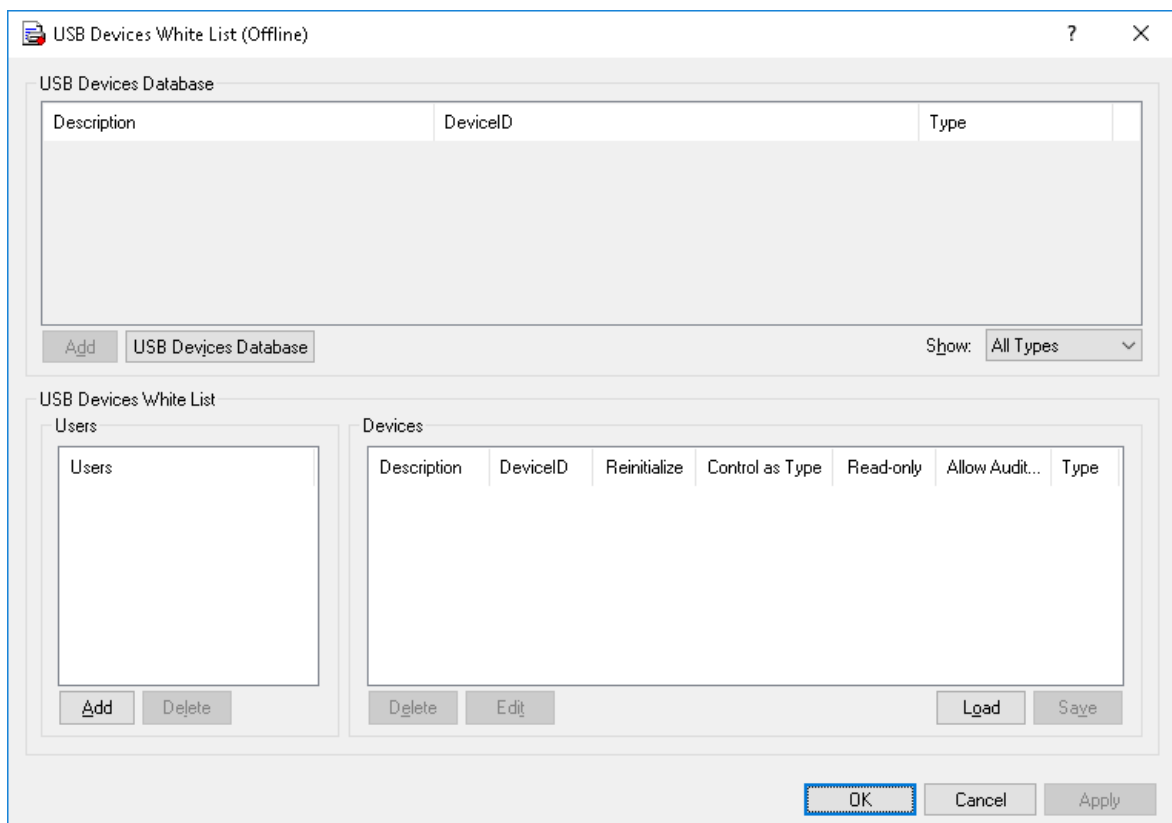
- [Defining and editing offline USB Devices White List](#)
- [Exporting and importing offline USB Devices White List](#)
- [Undefining offline USB Devices White List](#)
- [Removing offline USB Devices White List](#)

## Defining and editing offline USB Devices White List

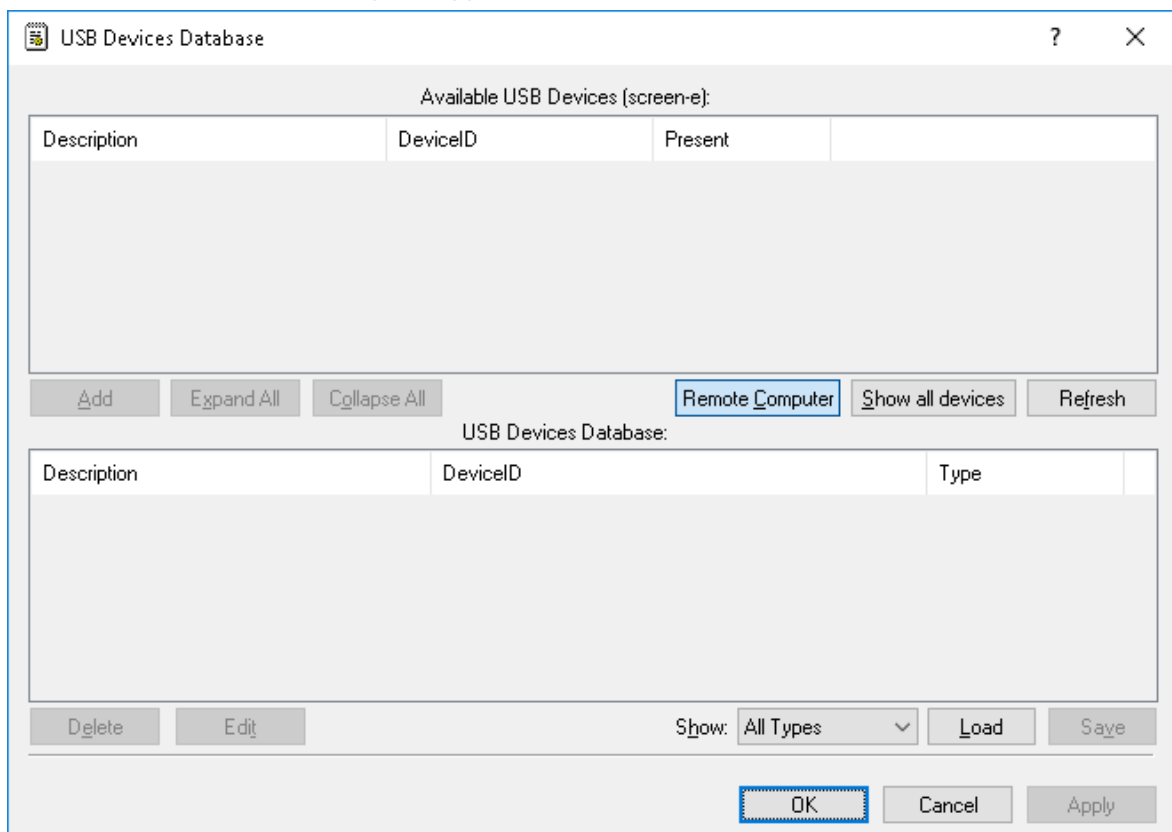
### ***To define and edit the offline USB Device White List***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **USB Devices White List**, and then click **Manage Offline**.  
- OR -
  - Select **USB Devices White List**, and then click **Manage Offline**  on the toolbar.

*The USB Devices White List (Offline) dialog box appears.*



4. In the upper pane of the **USB Devices White List (Offline)** dialog box, under **USB Devices Database**, click **USB Devices Database**.  
*The USB Devices Database dialog box appears.*



*In the upper pane of the USB Devices Database dialog box, under Available USB Devices, you can view the devices that are currently plugged in.*

To view all devices ever plugged into USB ports on the computer, click **Show all devices**. To view available devices on a remote computer, click **Remote Computer**.

*The Remote Computer button is unavailable when the management console is connected to the local computer.*

5. In the upper pane of the **USB Devices Database** dialog box, under **Available USB Devices**, select the device you want to add to the USB Devices White List, and then click **Add**.

*The device that you added is displayed under USB Devices Database in the lower pane of the dialog box.*

---

#### **Note**

You can add a device to the USB Devices White List only after you add this device to the USB Devices Database.

The same USB Devices Database is used for both the regular and offline USB Devices White List.

---

To delete a device from the USB Devices Database, in the lower pane of the **USB Devices Database** dialog box, under **USB Devices Database**, do one of the following:

- Select the device, and then click **Delete**.
  - OR -
- Right-click the device, and then click **Delete**.

*Devices are not deleted automatically from the white list after you delete them from the USB Devices Database.*

To edit a device's description, in the lower pane of the **USB Devices Database** dialog box, under **USB Devices Database**, select the device, and then click **Edit**.

*If you change a device's description in the USB Database, the following behavior occurs: The device will have its old description in the white list if it has already been added to the white list.*

6. Click **OK** or **Apply**.

*The device that you added to the USB Devices Database is displayed under USB Devices Database in the upper pane of the USB Devices White List (Offline) dialog box.*

7. In the lower-left pane of the **USB Devices White List (Offline)** dialog box, under **Users**, click **Add**.

*The Select Users or Groups dialog box appears.*

8. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the USB Devices White List, and then click **OK**.

*The users and groups that you added are displayed under Users in the lower-left pane of the USB Devices White List (Offline) dialog box.*

To delete a user or group, in the lower-left pane of the **USB Devices White List (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

9. In the lower-left pane of the **USB Devices White List (Offline)** dialog box, under **Users**, select the user or group.

*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*

10. In the upper pane of the **USB Devices White List (Offline)** dialog box, under **USB Devices Database**, select the device you want to add to the white list for the selected user or group, and then click **Add**.

*You can select multiple devices by holding down the SHIFT key or the CTRL key while clicking them.*

*The devices that you added to the white list are displayed under Devices in the lower-right pane of the dialog box.*

To delete a device from the white list for the selected user or group, in the lower-right pane of the **USB Devices White List (Offline)** dialog box, under **Devices**, do the following:

- Select the device, and then click **Delete**.
  - OR -
- Right-click the device, and then click **Delete**.
  - OR -
- Select the device, and then press the DELETE key.

To edit a device's description, in the lower-right pane of the **USB Devices White List (Offline)** dialog box, under **Devices**, do the following:

- Select the device, and then click **Edit**.
  - OR -
- Right-click the device, and then click **Edit**.

11. Click **OK** or **Apply**.


## Exporting and importing offline USB Devices White List

You can export the offline USB Devices White List to a .whl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.


### ***To export the offline USB Devices White List***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **USB Devices White List**, and then click **Save Offline**.
    - OR -



- Select **USB Devices White List**, and then click **Save Offline**  on the toolbar.
    - OR -
  - Expand **USB Devices White List**, right-click any user or group specified in the white list, and then click **Save Offline**.
    - OR -
  - Expand **USB Devices White List**, select any user or group specified in the white list. In the details pane, right-click the white listed device, and then click **Save**.
    - OR -
  - Right-click **USB Devices White List**, and then click **Manage Offline**. In the lower-right pane of the **USB Devices White List (Offline)** dialog box, under **Devices**, click **Save**.
4. In the **Save As** dialog box that appears, in the **Save in** box, browse to the location where you want to save the .whl file.
  5. In the **File name** box, type the file name you want.
  6. Click **Save**.
- When you export the offline USB Devices White List, it is saved in a file with a .whl extension.*

#### ***To import the offline USB Devices White List***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **USB Devices White List**, and then click **Load Offline**.
    - OR -
  - Select **USB Devices White List**, and then click **Load Offline**  on the toolbar.
    - OR -
  - Expand **USB Devices White List**, right-click any user or group specified in the white list, and then click **Load Offline**.
    - OR -
  - Expand **USB Devices White List**, and then select any user or group specified in the white list. In the details pane, right-click the white listed device, and then click **Load**.
    - OR -
  - Right-click **USB Devices White List**, and then click **Manage Offline**. In the lower-right pane of the **USB Devices White List (Offline)** dialog box, under **Devices**, click **Load**.

4. In the **Open** dialog box that appears, locate and select the file you want to import, and then click **Open**.

## Undefining offline USB Devices White List

You can return the previously defined offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.

### ***To undefine the offline USB Devices White List***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **USB Devices White List**, and then click **Undefine Offline**.  
*The offline state of the white list changes to "Not Configured."*  
When you select **USB Devices White List** in the console tree, in the details pane the following message is displayed: "Offline USB White List is not configured."

## Removing offline USB Devices White List

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of the higher-level offline white list and enforce the regular white list on specific lower-level groups of client computers. To enforce the regular USB Devices White List, the offline USB Devices White List must be removed.

### ***To remove the offline USB Devices White List***

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **USB Devices White List**, and then click **Remove Offline**.  
*The offline state of the white list changes to "Use Regular."*

When you select **USB Devices White List** in the console tree, in the details pane the following message is displayed: "Offline USB White List is configured to use Regular USB White List."

*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline Media White List

For details on the Media White List feature, see [Media White List \(Regular Profile\)](#).

The offline Media White List can have one of the following states:

- **Not Configured** - The white list is not defined. The following message is displayed: "Offline Media White List is not configured." This is the default state.
- **Configured** - The white list is defined.
- **Use Regular** - The inheritance of the offline white list is blocked and the regular white list is enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of the regular white list is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent the offline white list inherited from a higher level from being applied to a specific group of client computers at a lower level.

For more information on the enforcement of the regular white list, see [Removing offline Media White List](#).


Managing the offline Media White List involves the following tasks:

- [Defining and editing offline Media White List](#)
- [Exporting and importing offline Media White List](#)
- [Undefining offline media White List](#)
- [Removing offline Media White List](#)

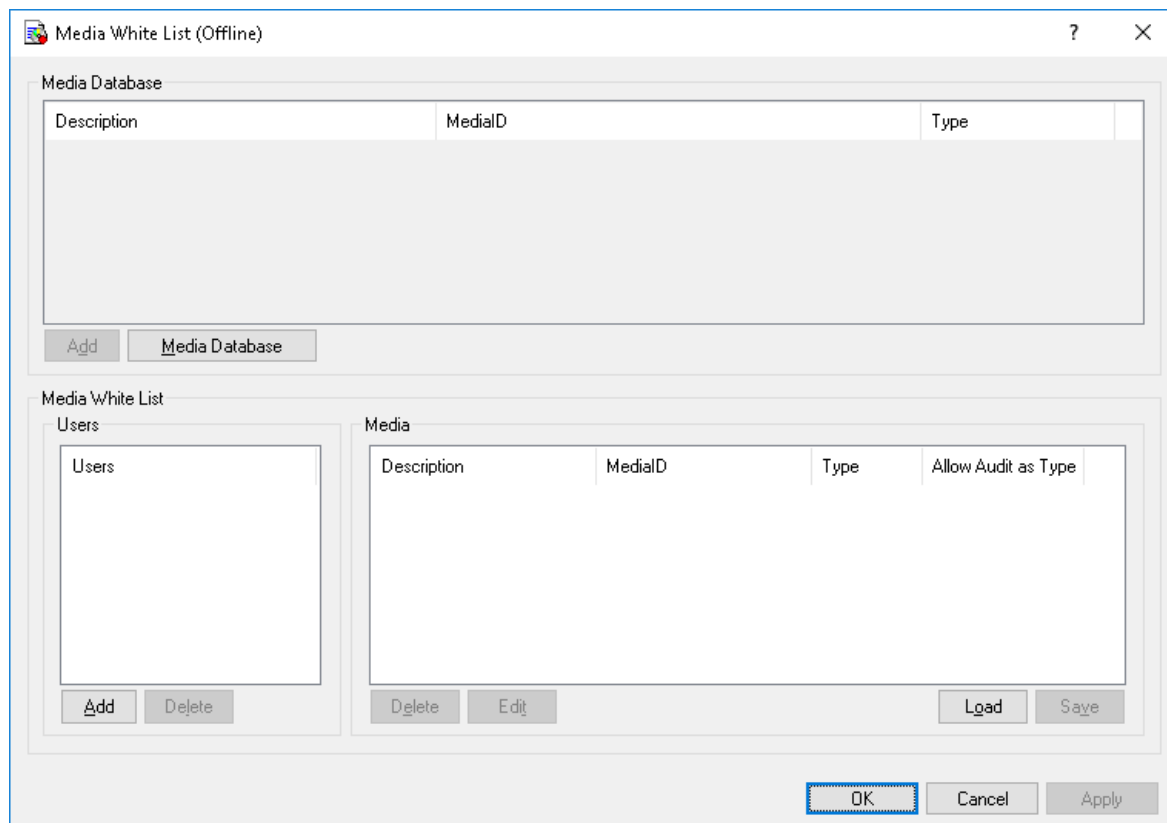
## Defining and editing offline Media White List

### ***To define and edit the offline Media White List***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.

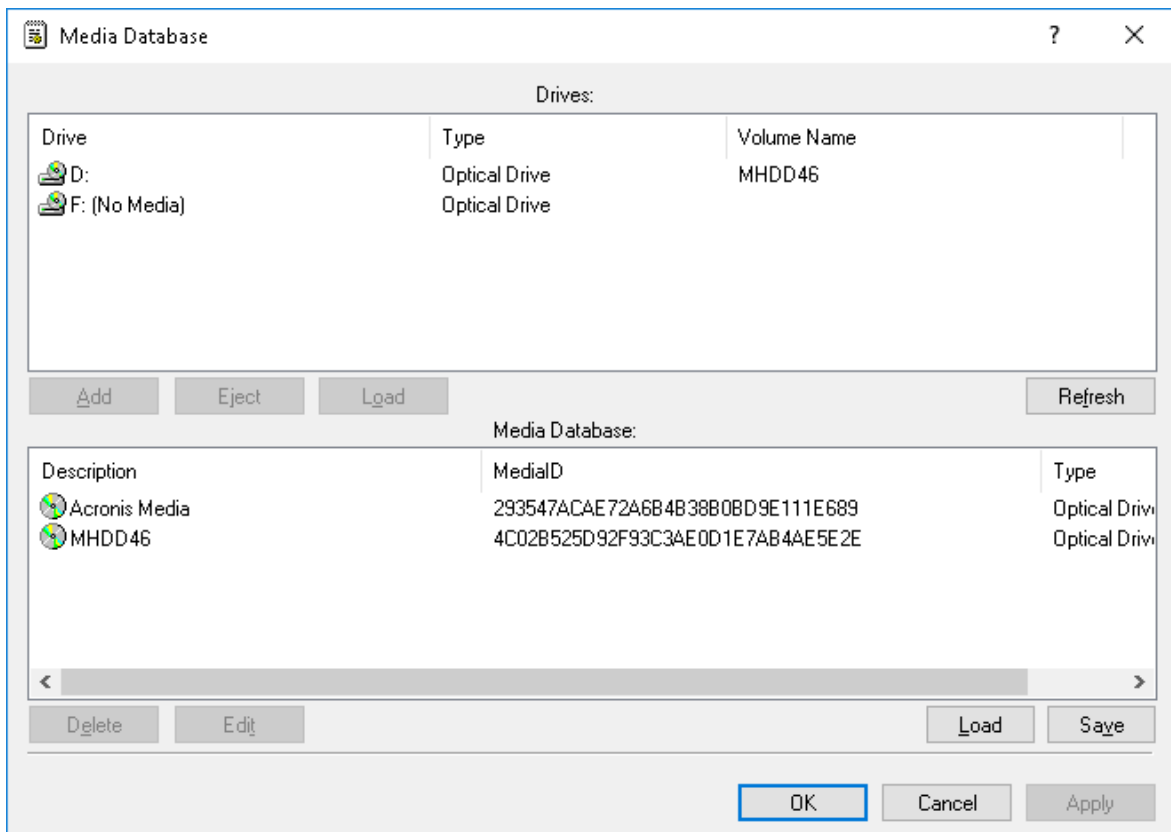
3. Under **Devices**, do one of the following:
- Right-click **Media White List**, and then click **Manage Offline**.
  - OR -
  - Select **Media White List**, and then click **Manage Offline**  on the toolbar.

*The Media White List (Offline) dialog box appears.*



4. In the upper pane of the **Media White List (Offline)** dialog box, under **Media Database**, click **Media Database**.

*The Media Database dialog box appears.*



In the upper pane of the **Media Database** dialog box, under **Drives**, you can view all CD/DVD/BD-ROM drives available on the local computer.

The list of drives is automatically refreshed and displays new media as soon as they arrive. To manually refresh this list, click **Refresh**.

5. In the upper pane of the **Media Database** dialog box, under **Drives**, select the drive that contains the media you want to add to the Media White List, and then click **Add**.  
The selected media are added to the Media Database and can be viewed in the lower pane of the **Media Database** dialog box.

#### Note

You can add media to the Media White List only after you add the media to the Media Database. The same Media Database is used for both the regular and offline Media White List.

To delete a medium from the white list, in the lower pane of the **Media Database** dialog box, do the following:

- Select the medium, and then click **Delete**.  
- OR -
- Right-click the medium, and then click **Delete**.

To edit a medium's description, in the lower pane of the **Media Database** dialog box, select the medium, and then click **Edit**.

6. Click **OK** or **Apply**.  
The media that you added to the Media Database are displayed under Media Database in the upper pane of the **Media White List (Offline)** dialog box.


7. In the lower-left pane of the **Media White List (Offline)** dialog box, under **Users**, click **Add**.
8. In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the Media White List, and click **OK**.  
*The users and groups that you added are displayed under Users in the lower-left pane of the Media White List (Offline) dialog box.*  
 To delete a user or group, in the lower-left pane of the **Media White List (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.
9. In the lower-left pane of the **Media White List (Offline)** dialog box, under **Users**, select the user or group.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
10. In the upper pane of the **Media White List (Offline)** dialog box, under **Media Database**, select the medium you want to add to the white list for the selected user or group, and then click **Add**.  
*You can select multiple media by holding down the SHIFT key or the CTRL key while clicking them.*  
*The media that you added to the white list are displayed under Media in the lower-right pane of the dialog box.*  
 To delete a medium from the white list for the selected user or group, in the lower-right pane of the **Media White List (Offline)** dialog box, under **Media**, do the following:
  - Select the medium, and then click **Delete**.
  - OR -
  - Right-click the medium, and then click **Delete**.
 To edit a medium's description for the selected user or group, in the lower-right pane of the **Media White List (Offline)** dialog box, under **Media**, do the following:
  - Select the medium, and then click **Edit**.
  - OR -
  - Right-click the medium, and then click **Edit**.
11. Click **OK** or **Apply**.

## Exporting and importing offline Media White List


You can export the offline Media White List to a .mwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

### **To export the offline Media White List**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Group Policy Manager, do the following:

- a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **Media White List**, and then click **Save Offline**.  
- OR -
  - Select **Media White List**, and then click **Save Offline**  on the toolbar.  
- OR -
  - Expand **Media White List**, right-click any user or group specified in the white list, and then click **Save Offline**.  
- OR -
  - Expand **Media White List**, and then select any user or group specified in the white list. In the details pane, right-click the white listed medium, and then click **Save**.  
- OR -
  - Right-click **Media White List**, and then click **Manage Offline**. In the lower-right pane of the **Media White List (Offline)** dialog box, under **Media**, click **Save**.
4. In the **Save As** dialog box that appears, in the **Save in** box, browse to the location where you want to save the .mwl file.
5. In the **File name** box, type the file name you want.
6. Click **Save**.  
*When you export the offline Media White List, it is saved in a file with a .mwl extension.*

### **To import the offline Media White List**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **Media White List**, and then click **Load Offline**.  
- OR -
  - Select **Media White List**, and then click **Load Offline**  on the toolbar.  
- OR -
  - Expand **Media White List**, right-click any user or group specified in the white list, and then click **Load Offline**.

- OR -
  - Expand **Media White List**, and then select any user or group specified in the white list. In the details pane, right-click the white listed device, and then click **Load**.
  - OR -
  - Right-click **Media White List**, and then click **Manage Offline**. In the lower-right pane of the **Media White List (Offline)** dialog box, under **Media**, click **Load**.
4. In the **Open** dialog box that appears, in the **Look in** list, click the location that contains the file you want to import.
  5. In the folder list, locate and open the folder that contains the file.
  6. Click the file, and then click **Open**.

## Undefined offline media White List

You can return the previously defined offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.

### ***To undefine the offline Media White List***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **Media White List**, and then click **Undefine Offline**.  
*The offline state of the white list changes to "Not Configured."*  
When you select **Media White List** in the console tree, in the details pane the following message is displayed: "Offline Media White List is not configured."

## Removing offline Media White List

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of the higher-level offline white list and enforce the regular white list on specific lower-level groups of client computers. To enforce the regular Media White List, the offline Media White List must be removed.

### ***To remove the offline Media White List***



1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **Media White List**, and then click **Remove Offline**.  
*The offline state of the white list changes to "Use Regular."*  
When you select **Media White List** in the console tree, in the details pane the following message is displayed: "Offline Media White List is configured to use Regular Media White List."  
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline Content-Aware Rules for Devices

For details on the Content-Aware Rules feature for devices, see [Rules for Devices](#) in [Content-Aware Rules \(Regular Profile\)](#).

The offline Content-Aware Rules can have one of the following states:

- **Not Configured** - Content-Aware Rules are not defined. The following message is displayed: "Offline Content-Aware Rules are not configured." This is the default state.
- **Configured** - Content-Aware Rules are defined.
- **Use Regular** - The inheritance of offline Content-Aware Rules is blocked and regular Content-Aware Rules are enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of regular Content-Aware Rules is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent offline Content-Aware Rules inherited from a higher level from being applied to a specific group of client computers at a lower level.  
For more information on the enforcement of regular Content-Aware Rules, see [Removing offline Content-Aware Rules](#).

Managing offline Content-Aware Rules involves the following tasks:

- [Defining offline Content-Aware Rules](#)
- [Editing offline Content-Aware Rules](#)
- [Copying offline Content-Aware Rules](#)
- [Exporting and importing offline Content-Aware Rules](#)
- [Deleting offline Content-Aware Rules](#)
- [Undefining offline Content-Aware Rules](#)
- [Removing offline Content-Aware Rules](#)


## Defining offline Content-Aware Rules

Content-Aware Rules are created based on either the built-in or custom content groups. For detailed information on these groups, see [Configuring Content Groups](#).

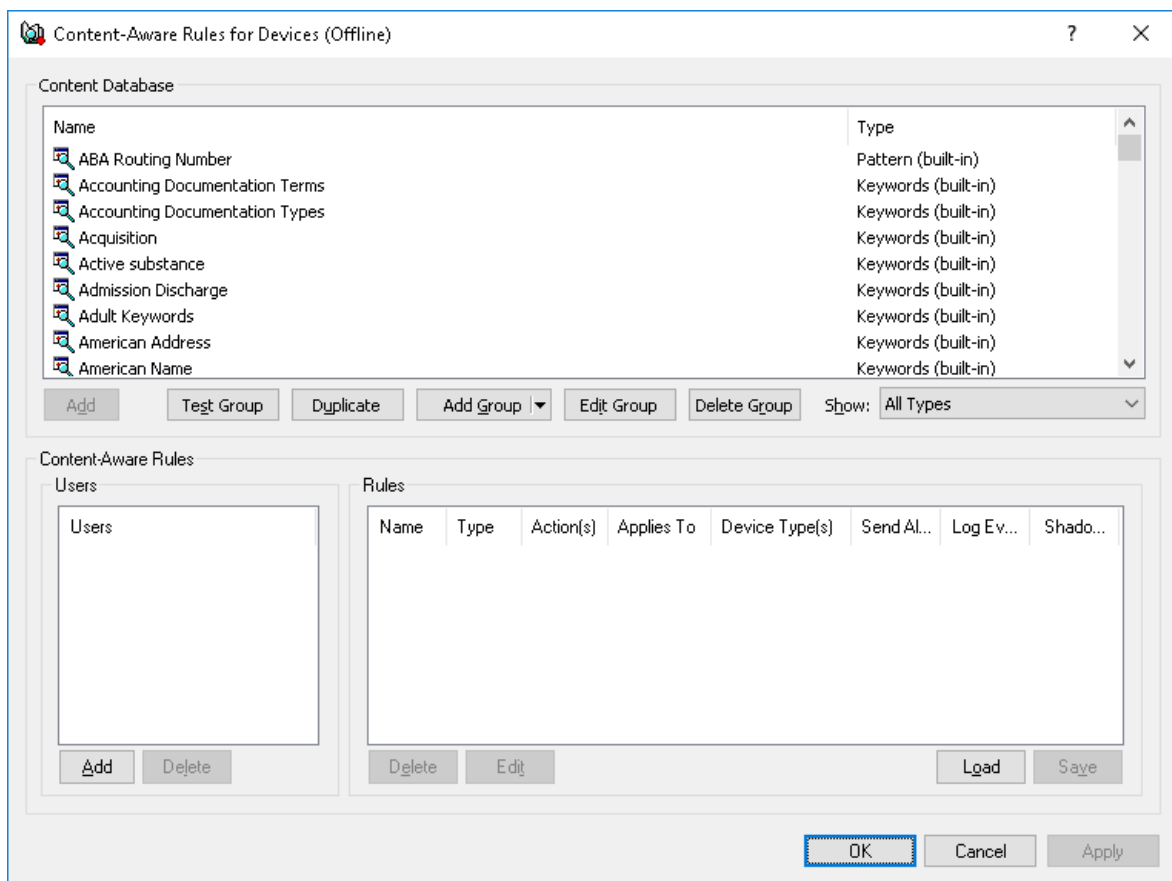
You can enable offline alerts that are sent when a specific offline Content-Aware Rule fires. Such alerts are enabled immediately after setting up an offline Content-Aware Rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific Content-Aware Rule, alert settings must be configured in DeviceLock Service options (see [Alerts](#)).

### ***To define an offline Content-Aware Rule***

1. If using the DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage Offline**.  
- OR -
  - Select **Content-Aware Rules**, and then click **Manage Offline**  on the toolbar.

*The Content-Aware Rules for Devices (Offline) dialog box appears.*



4. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, click **Add**.

*The Select Users or Groups dialog box appears.*

5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the rule, and then click **OK**.  
*The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Devices (Offline) dialog box.*

To delete a user or group, in the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

6. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the users or groups for which you want to define the rule.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
7. In the upper pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Content Database**, select the desired content group, and then click **Add**, or double-click the desired content group.

---

### Note

You can specify only one content group for a Content-Aware Rule.

---

*The Add Rule dialog box appears.*

**Add Rule**

Name:

Applies to

☐ Permissions ☐ Shadowing ☐ Detection

If this rule triggers

☐ Send Alert ☐ Log Event ☐ Shadow Copy

Devices Type(s):

Actions

	Allow	Deny
User's Rights		

View Group OK Cancel

8. In the **Add Rule** dialog box, in the **Name** box, type the name of the Content-Aware Rule. By default, the rule has the same name as its content group. The name of the rule can be changed if needed.  
To view this rule's content group, click the **View Group** button in the bottom left corner of the dialog box. The console displays the properties of the group in a separate dialog box, allowing property values to be viewed but not modified.
9. Under **Applies to**, specify the type of operation associated with the rule. The available options are:
  - **Permissions** - Specifies that the rule will apply to access control operations.
  - **Shadowing** - Specifies that the rule will apply to shadow copy operations.
  - **Detection** - Specifies that the rule will apply to detection operations.
  - **Permissions, Shadowing** - Specifies that the rule will apply to both access control and shadow copy operations.
  - **Permissions, Detection** - Specifies that the rule will apply to both access control and detection operations.

- **Shadowing, Detection** - Specifies that the rule will apply to both shadow copy and detection operations.
- **Permissions, Shadowing, Detection** - Specifies that the rule will apply to all available operations: access control, shadow copy, and detection.

---

#### Note

To successfully create/save a rule that applies either to detection operations only or to detection operations combined with other operations, at least one of the following options must be selected for this rule: **Log Event**, **Send Alert** or **Shadow Copy** (see step 10 of this procedure). Otherwise, the rule cannot be saved and the following message appears: "Log Event, Send Alert or Shadow Copy should be specified."

---

- Under **If this rule triggers**, specify the following additional actions to be performed when the rule triggers:

- **Send Alert** - Specifies that an alert is sent whenever the rule triggers.
- **Log Event** - Specifies that an event is logged in the Audit Log whenever the rule triggers.
- **Shadow Copy** - Specifies that a shadow copy of data is created whenever the rule triggers.

When alerts, audit and/or shadowing are enabled or disabled in a Content-Aware Rule, the rule setting takes precedence over the respective setting for the device type.

Example: If audit is enabled for a particular device type and disabled in a rule for that device type, the triggering of the rule does not cause audit events. If audit is enabled in the rule, then the triggering of the rule causes audit events, even if audit is disabled at the device-type level.

The rule can also inherit the alert, audit and/or shadowing setting from the device-type level. This is the default option, represented by the indeterminate state of the check boxes (neither checked nor cleared). The state of each check box can be changed individually.

Example: When a rule inherits the audit setting from the device-type level, the triggering of the rule causes audit events only if audit is enabled for the device type controlled by that rule.

- Under **Device Type(s)**, select the appropriate device type(s) you would like this rule to be applied to.

*Content-Aware Rules can be applied to the following device types: Clipboard, Floppy, iPhone, MTP, Optical Drive, Palm, Printer, Removable, TS Devices, and Windows Mobile.*

- Under **Action(s)**, specify which user actions are allowed or disallowed on files, which user actions are logged to the shadow log, and which user actions are detected.

If the rule applies to shadow copy operations combined with other operations, the Read user right becomes unavailable. If the rule applies to detection operations combined with other operations, only Allow action becomes available. For detailed information on user rights and actions that can be specified in Content-Aware Rules, see [Access Control](#), [Content-Aware Shadowing](#) and [Content-Aware Detection](#) for devices.

- Click **OK**.

*The rule you created is displayed under Rules in the lower-right pane of the Content-Aware Rules for Devices (Offline) dialog box.*

14. Click **OK** or **Apply** to apply the rule.

*The users or groups to which the Content-Aware Rule applies are displayed under Content-Aware Rules in the console tree.*

When you select a user or group to which a Content-Aware Rule applies in the console tree, in the details pane you can view detailed information regarding this rule (see [List of Content-Aware Rules for Devices](#)).

You can define different online vs. offline Content-Aware Rules for the same user or sets of users. For information on how to define online Content-Aware Rules, see [Managing Content-Aware Rules in Content-Aware Rules \(Regular Profile\)](#).

## Editing offline Content-Aware Rules

You can modify the Content-Aware Rule properties such as **Name**, **Applies To**, **If this rule triggers**, **Device Type(s)**, **Actions**.

### **To edit an offline Content-Aware Rule**


1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **Content-Aware Rules**, click **Manage Offline**, and then do the following:
  - a. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.*
  - b. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.  
- OR -  
Right-click the rule, and then click **Edit**.  
- OR -  
Double-click the rule.  
- OR -  
Under **Devices**, expand **Content-Aware Rules**, and then do the following:

- a. Under **Content-Aware Rules**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them in the details pane.*
  - c. In the details pane, right-click the rule you want to edit, and then click **Edit**.  
*The Edit Rule dialog box appears.*
4. In the **Edit Rule** dialog box, modify the rule properties as required to meet your needs.
5. Click **OK** to apply the changes.

## Copying offline Content-Aware Rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing offline Content-Aware Rules.

### To copy an offline Content-Aware Rule


1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage Offline**.  
- OR -
  - Select **Content-Aware Rules**, and then click **Manage Offline**  on the toolbar.  
*The Content-Aware Rules for Devices (Offline) dialog box appears.*
4. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.*
5. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.  
*The rule you cut or copy is automatically copied to the Clipboard.*  
*You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you cut the rule, the rule will be cut only after you paste it.*  
To perform a drag-and-drop operation, select the rule and move it to the user or group to which you want to apply the copied rule.

6. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.  
*The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Devices (Offline) dialog box.*
8. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the users or groups for which you want to set permissions.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
9. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, right-click in the **Rules** pane and then click **Paste**.  
*The copied rule is displayed under Rules in the lower-right pane of the Content-Aware Rules for Devices (Offline) dialog box.*
10. Click **OK** or **Apply** to apply the copied rule.


## Exporting and importing offline Content-Aware Rules

You can export all your current offline Content-Aware Rules to a .cwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.



### To export offline Content-Aware Rules

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Save Offline**.  
- OR -
  - Select **Content-Aware Rules**, and then click **Save Offline**  on the toolbar.  
- OR -
  - Expand **Content-Aware Rules**, right-click any user or group, and then click **Save Offline**.  
- OR -
  - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Save**.



- OR -
  - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Save Offline**  on the toolbar.
  - OR -
  - Right-click **Content-Aware Rules**, and then click **Manage (Offline)**. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, click **Save**.
4. In the **Save As** dialog box that appears, choose the folders where you want to save the .cwl file, specify the files name, and then click **Save**.
- When you export rules, they are saved in a file with a .cwl extension.*

### **To import offline Content-Aware Rules**

1. If using DeviceLock Management Console, do the following:
    - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
    - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
      - a. Open DeviceLock Service Settings Editor.
    - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
      - a. Open Group Policy Object Editor.
    - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
  2. Expand **Devices**.
  3. Under **Devices**, do one of the following:
    - Right-click **Content-Aware Rules**, and then click **Load Offline**.
    - OR -
    - Select **Content-Aware Rules**, and then click **Load Offline**  on the toolbar.
    - OR -
    - Expand **Content-Aware Rules**, right-click any user or group, and then click **Load Offline**.
    - OR -
    - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Load**.
    - OR -
    - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Load Offline**  on the toolbar.
    - OR -
    - Right-click **Content-Aware Rules**, and then click **Manage Offline**. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, click **Load**.
  4. In the **Open** dialog box that appears, locate and select the file you want to import, and then click **Open**.
- You can import only one .cwl file at a time.*

## Deleting offline Content-Aware Rules

You can delete individual offline Content-Aware Rules when they are no longer required.

### **To delete an offline Content-Aware Rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Expand **Content-Aware Rules**, right-click the user or group to which the rule is applied, and then click **Delete user**.  
*When you delete a user or group, the rule associated with this user or group is automatically deleted.*  
- OR -
  - Expand **Content-Aware Rules**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.  
- OR -
  - Right-click **Content-Aware Rules**, and then click **Manage Offline**. In the lower-left pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Users**, select the user or group to which the rule is applied. In the lower-right pane of the **Content-Aware Rules for Devices (Offline)** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.  
*You can select multiple rules that you want to delete by holding down the SHIFT key or the CTRL key while clicking them.*

## Undefined offline Content-Aware Rules

You can return the previously defined offline Content-Aware Rules to the unconfigured state. If offline rules are undefined, regular rules are applied to offline client computers.

### **To undefine offline Content-Aware Rules**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.

- b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
  3. Under **Devices**, right-click **Content-Aware Rules**, and then click **Undefine Offline**.  
*The offline state of Content-Aware Rules changes to "Not Configured."*  
When you select **Content-Aware Rules** in the console tree, in the details pane the following message is displayed: "Offline Content-Aware Rules are not configured."

## Removing offline Content-Aware Rules

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline Content-Aware Rules and enforce regular Content-Aware Rules on specific lower-level groups of client computers. To enforce regular Content-Aware Rules, offline Content-Aware Rules must be removed.

### **To remove offline Content-Aware Rules**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, right-click **Content-Aware Rules**, and then click **Remove Offline**.  
*The offline state of Content-Aware Rules changes to "Use Regular."*  
When you select **Content-Aware Rules** in the console tree, in the details pane the following message is displayed: "Offline Content-Aware Rules are configured to use Regular Content-Aware Rules."  
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline Security Settings for Devices

For details on the Security Settings feature, see [Security Settings \(Regular Profile\)](#).

Offline Security Settings can have one of the following states:

- **Not Configured** - Security Settings are not defined. This is the default state.
- **Enabled** - Security Settings are defined to enable audit and access control for the specified device classes.
- **Disabled** - Security Settings are defined to disable audit and access control for the specified device classes.
- **Use Regular** - The inheritance of offline Security Settings is blocked and regular Security Settings are enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of regular Security Settings is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent offline Security Settings inherited from a higher level from being applied to a specific group of client computers at a lower level.  
For more information on the enforcement of regular Security Settings, see [Removing offline Security Settings](#).

Managing offline Security Settings involves the following tasks:

- [Defining and changing offline Security Settings](#)
- [Undefining offline Security Settings](#)
- [Removing offline Security Settings](#)


## Defining and changing offline Security Settings

Offline Security Settings can be defined and changed individually or collectively.

### ***To define and change offline Security Settings individually***

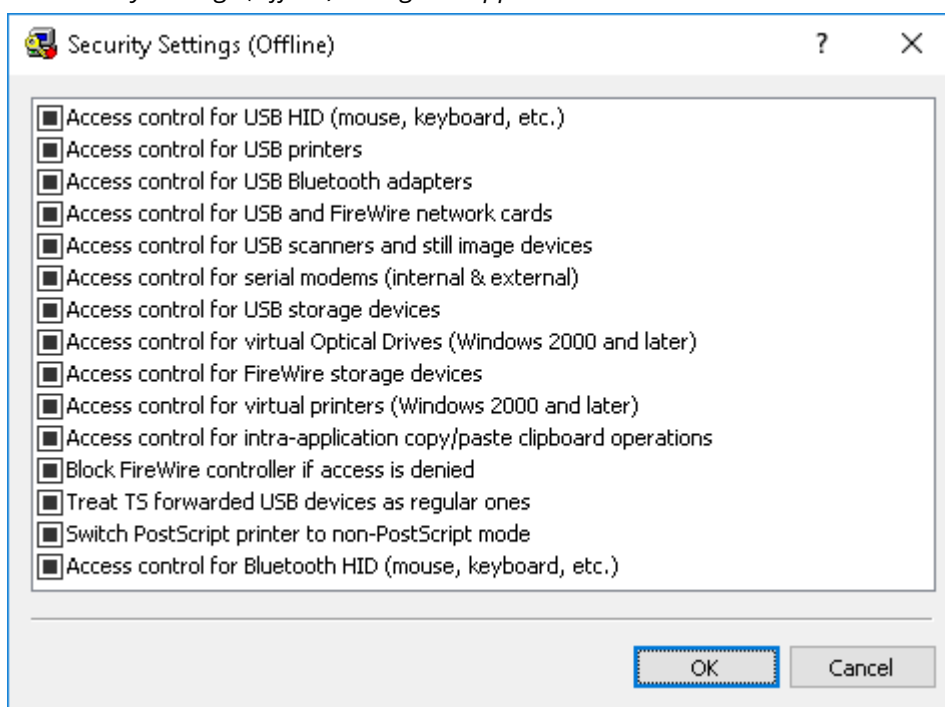
1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Security Settings**.  
*When you select Security Settings in the console tree, they are displayed in the details pane.*
4. In the details pane, right-click any Security Setting, and then click **Enable Offline**.  
*The Security Setting changes its offline state from "Not Configured" to "Enabled."*  
Once you have enabled a particular Security Setting, you can disable it. To do so, right-click the enabled Security Setting, and then click **Disable Offline**.  
*The Security Setting changes its offline state from "Enabled" to "Disabled."*

### ***To define and change offline Security Settings collectively***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **Security Settings**, and then click **Manage Offline**.  
- OR -
  - Select **Security Settings**, and then click **Manage Offline**  on the toolbar.  
- OR -
  - Select **Security Settings**. In the details pane, right-click any Security Setting, and then click **Manage Offline**.  
- OR -
  - Select **Security Settings**. In the details pane, select any Security Setting, and then click **Manage Offline**  on the toolbar.

*When you select Security Settings in the console tree, they are displayed in the details pane.*

*The Security Settings (Offline) dialog box appears.*



4. In the **Security Settings (Offline)** dialog box, select the appropriate check boxes for the Security Settings that you want to define.  
*Once you have enabled Security Settings, you can disable them. To do so, clear the appropriate check boxes.*

---

**Note**

All check boxes in the **Security Settings (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of Security Settings.

---

5. Click **OK**.

## Undefining offline Security Settings



You can return the previously defined offline Security Settings to the unconfigured state. If offline Security Settings are undefined, regular Security Settings are applied to offline client computers. You can undefine Security Settings individually or collectively.

### ***To undefine offline Security Settings individually***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, select **Security Settings**.  
*When you select Security Settings in the console tree, they are displayed in the details pane.*
4. In the details pane, right-click any Security Setting you want to undefine, and then click **Undefine Offline**.  
*The Security Setting changes its offline state to "Not Configured."*

### ***To undefine offline Security Settings collectively***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.

- c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
  - a. Open Group Policy Object Editor.
- d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.
3. Under **Devices**, do one of the following:
  - Right-click **Security Settings**, and then click **Manage Offline**.  
- OR -
  - Select **Security Settings**, and then click **Manage Offline**  on the toolbar.  
- OR -
  - Select **Security Settings**. In the details pane, right-click any Security Setting, and then click **Manage Offline**.  
- OR -
  - Select **Security Settings**. In the details pane, select any Security Setting, and then click **Manage Offline**  on the toolbar.

*When you select Security Settings in the console tree, they are displayed in the details pane.*  
*The Security Settings (Offline) dialog box appears.*
4. In the **Security Settings (Offline)** dialog box, return the appropriate check boxes to the indeterminate state.

---

**Note**

All check boxes in the **Security Settings (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of Security Settings.

---

## Removing offline Security Settings

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline Security Settings and enforce regular Security Settings on specific lower-level groups of client computers. To enforce regular Security Settings, offline Security Settings must be removed. The console allows you to remove only individual Security Settings one by one.

### **To remove offline Security Settings**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Devices**.

3. Under **Devices**, select **Security Settings**.  
*When you select Security Settings in the console tree, they are displayed in the details pane.*
4. In the details pane, right-click the Security Setting to remove, and then click **Remove Offline**.  
*The Security Setting changes its offline state to "Use Regular."*  
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline Security Policies for Protocols

Managing offline security policies for protocols involves the following operations:

- [Managing Offline Permissions for Protocols](#)
- [Managing Offline Audit, Shadowing and Alerts for Protocols](#)
- [Managing Offline Protocols White List](#)
- [Managing Offline IP Firewall](#)
- [Managing Offline Content-Aware Rules for Protocols](#)
- [Managing Offline Security Settings for Protocols](#)

You can manage offline security policies by using DeviceLock Management Console, Service Settings Editor, or DeviceLock Group Policy Manager.

## Managing Offline Permissions for Protocols

For details on the Permissions feature for protocols, see [Managing Permissions for Protocols](#).

Offline permissions can have one of the following states:

- **Not Configured** - No permission settings are specified for the protocol.
- **Configured** - Different accounts are assigned different permissions for the protocol.
- **Full Access** - All accounts have full access to the protocol.  
This state shows up, for example, when permissions are set only for the "Everyone" account so that it has full access to the protocol.
- **No Access** - No accounts have access to the protocol.  
This state shows up, for example, when the "Everyone" account is explicitly denied any access to the protocol, or permissions are not set for any accounts. Note that the denial for the "Everyone" account overrides any permissions for other accounts.
- **Use Regular** - Inheritance of offline permissions is blocked and regular permissions are enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of regular permissions is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent offline permissions inherited from a higher level from being applied to a specific group of client computers at a lower level.  
For more information on the enforcement of regular permissions, see [Removing offline permissions](#).




Managing offline permissions involves the following tasks:

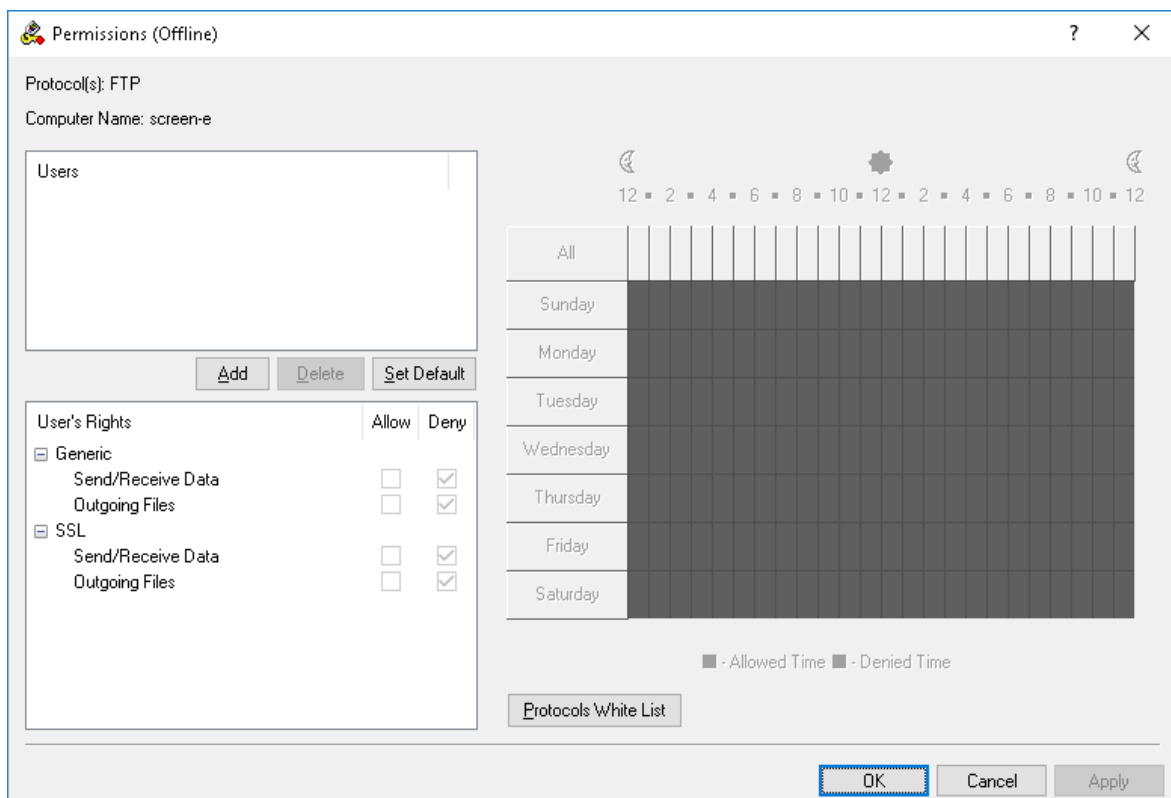
- [Setting and editing offline permissions](#)
- [Undefining offline permissions](#)
- [Removing offline permissions](#)

## Setting and editing offline permissions

### ***To set and edit offline permissions***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.  
*When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions. In the details pane, you can also view the current state of offline permissions for each protocol in the Offline column.*
4. In the details pane, do one of the following:
  - Right-click the protocol for which you want to set or edit permissions, and then click **Set Offline Permissions**.  
- OR -
  - Select the protocol for which you want to set or edit permissions, and then click **Set Offline Permissions**  on the toolbar.

*The Permissions (Offline) dialog box appears.*



5. In the **Permissions (Offline)** dialog box, do the following:

**To set the default permissions**

- In the upper-left pane of the dialog box, under **Users**, click **Set Default**.  
The default permissions are assigned to the Administrators and Everyone accounts. For information about which permissions are set for these accounts by default, see [Managing Permissions for Protocols](#).

**To set permissions for an additional user or group**

- In the upper-left pane of the dialog box, under **Users**, click **Add**.
- In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.  
*The users and groups that you added are displayed under Users in the upper-left pane of the Permissions (Offline) dialog box.*
- In the upper-left pane of the **Permissions (Offline)** dialog box, under **Users**, select the user or group.  
*You can select multiple users and/ or groups by holding down the SHIFT key or the CTRL key while clicking them.*
- In the lower-left pane of the **Permissions (Offline)** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights.  
*In the right pane of the Permissions (Offline) dialog box, you can set day and time restrictions that narrow user access to the specified protocol(s). Use the left mouse button to select days and hours when the selected user or group will have access to the specified protocol(s). Use the right mouse button to mark days and hours when the selected user or group will not have access to the specified protocol(s).*

### To change permissions for an existing user or group

- a. In the upper-left pane of the dialog box, under **Users**, select the user or group.
- e. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate access rights.

### To remove an existing user or group and permissions

- In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.

*When you remove a user or group, any permissions for that user or group will also be removed.*

### To set, view, or change Protocols White List rules for this protocol

- Click the **Protocols White List** button. For further details on the Protocols White List for offline mode, see [Managing Offline Protocols White List](#).

### To set, view, or change Security Settings for the MAPI protocol

- Click the **Security Settings** button. For further details on the protocol Security Settings for offline mode, see [Managing Offline Security Settings for Protocols](#).

---

#### Note

The **Permissions (Offline)** dialog box displays the **Security Settings** button only when managing permissions for the MAPI protocol. For other protocols, this button is not available.

---

6. Click **OK** or **Apply**.

## Undefining offline permissions

You can reset previously set offline permissions to the unconfigured state. If offline permissions are undefined, regular permissions are applied to offline client computers.

### To undefine offline permissions

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.

*When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions. In the details pane you can also view the current state of offline permissions for each protocol in the Offline column.*

4. In the details pane, right-click the protocol for which you want to undefine offline permissions, and then click **Undefine Offline**.

*You can undefine offline permissions set for several protocols at the same time. To do this, do the following:*

- a. In the details pane, select several protocols by holding down the SHIFT key or the CTRL key while clicking them.
- b. Right-click the selection, and then click **Undefine Offline**.

*The offline state of the permissions changes to "Not Configured."*

## Removing offline permissions

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline permissions and enforce regular permissions on specific lower-level groups of client computers. To enforce regular permissions, offline permissions must be removed.

### **To remove offline permissions**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Permissions**.  
*When you select Permissions in the console tree, in the details pane you can view protocols for which you can set permissions. In the details pane you can also view the current state of offline permissions for each protocol in the Offline column.*
4. In the details pane, right-click the protocol for which you want to remove offline permissions, and then click **Remove Offline**.  
*You can remove offline permissions set for several protocols at the same time. To do this, do the following:*
  - a. In the details pane, select several protocols by holding down the SHIFT key or the CTRL key while clicking them.
  - b. Right-click the selection and then click **Remove Offline**.  
*The offline state of the permissions changes to "Use Regular."*  
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline Audit, Shadowing and Alerts for Protocols

For details on the Auditing & Shadowing feature for protocols, see [Managing Audit, Shadowing and Alerts for Protocols](#). For details on the Alerts feature, see [Alerts](#). For information about how to

enable online (regular) alerts, see [Managing Audit, Shadowing and Alerts for Protocols](#). For information about how to enable offline alerts, see [Enabling offline alerts](#).

Offline audit, shadowing rules and alerts can have one of the following states:

- **Not Configured** - Offline audit, shadowing rules, and alerts are not defined for the protocol.
- **Configured** - Offline audit, shadowing rules and/or alerts are defined for the protocol.
- **No Audit** - Offline settings for the protocol do not allow audit, shadowing, and alerts for any accounts.
- **Use Regular** - Inheritance of offline audit and shadowing rules is blocked and regular audit and shadowing rules are enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of regular rules is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent offline rules inherited from a higher level from being applied to a specific group of client computers at a lower level.

For more information on the enforcement of regular rules, see [Removing offline audit and shadowing rules](#).


Managing offline audit, shadowing rules and alerts involves the following tasks:

- [Defining and editing offline audit and shadowing rules](#)
- [Enabling offline alerts](#)
- [Undefined offline audit and shadowing rules](#)
- [Removing offline audit and shadowing rules](#)

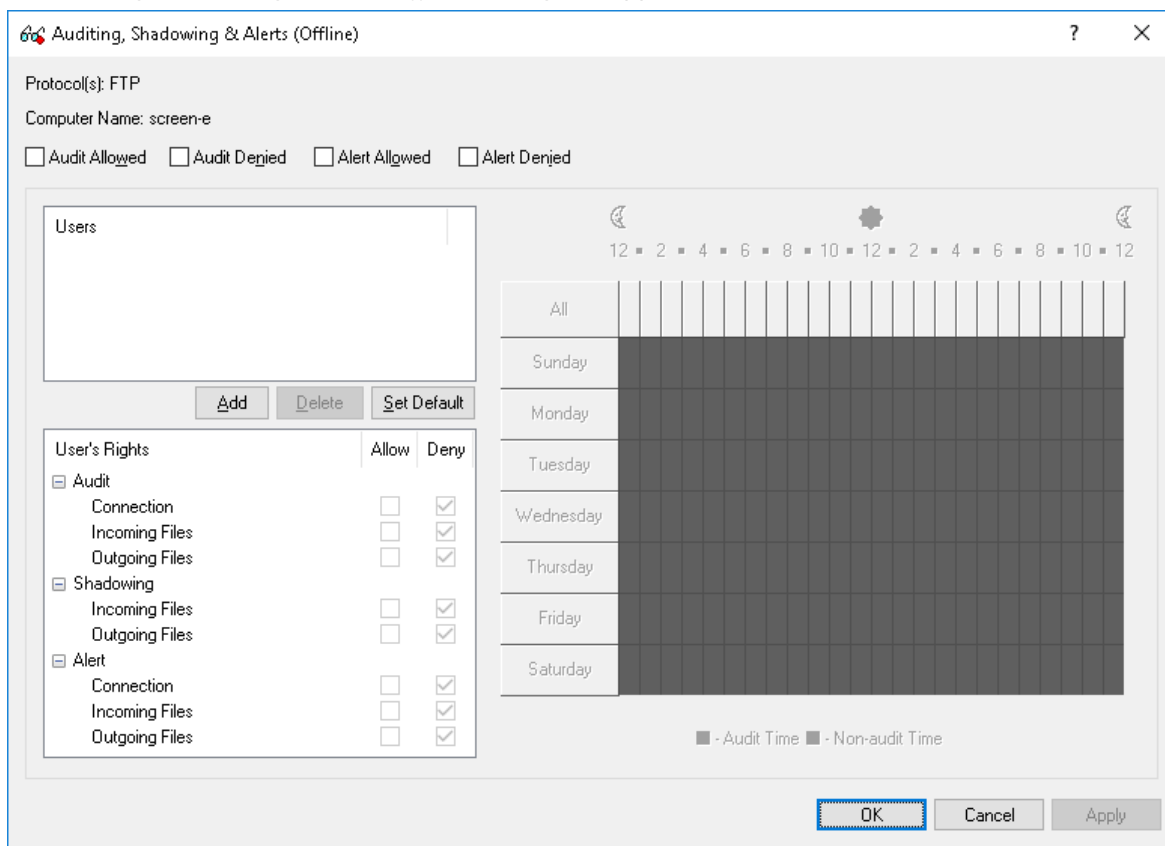
## Defining and editing offline audit and shadowing rules

### ***To define and edit offline audit and shadowing rules***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.  
*When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each protocol in the Offline column.*

4. In the details pane, do one of the following:
  - Right-click the protocol for which you want to define or edit rules, and then click **Set Offline Auditing, Shadowing & Alerts**.
  - OR -
  - Select the protocol for which you want to define or edit rules, and then click **Set Offline Auditing, Shadowing & Alerts**  on the toolbar.

The *Auditing, Shadowing & Alerts (Offline)* dialog box appears.



5. In the **Auditing, Shadowing & Alerts (Offline)** dialog box, do the following:
 

**To define the default audit and shadowing rules**

  - a. In the upper-left area of the dialog box, specify which events are written to the Audit Log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a protocol. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a protocol.
  - b. In the upper-left pane of the dialog box, under **Users**, click **Set Default**. The default audit and shadowing rules apply to the Users and Everyone groups. For information about which Audit and Shadowing rights are set for these groups by default, see [Managing Audit, Shadowing and Alerts for Protocols](#).

**To define audit and shadowing rules for an additional user or group**

  - a. In the upper-left area of the dialog box, specify which events are written to the Audit Log. Select the **Audit Allowed** check box to audit successful attempts to gain access to a protocol. Select the **Audit Denied** check box to audit unsuccessful attempts to gain access to a protocol.

- c. In the upper-left pane of the dialog box, under **Users**, click **Add**.
  - d. In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.  
*The users and groups that you added are displayed under Users in the upper-left pane of the Auditing, Shadowing & Alerts (Offline) dialog box.*
  - e. In the upper-left pane of the **Auditing, Shadowing & Alerts (Offline)** dialog box, under **Users**, select the user or group.  
*You can select multiple users and/or groups by holding down the SHIFT key or the CTRL key while clicking them.*
  - f. In the lower-left pane of the **Auditing, Shadowing & Alerts (Offline)** dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate audit and shadowing rights.  
*Audit and Shadowing rights determine which user actions on protocols are logged to the Audit and/or Shadow Log.*  
*In the right pane of the Auditing, Shadowing & Alerts (Offline) dialog box, you can specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on protocols will be logged to either the Audit or Shadow Log. Use the left mouse button to select days and hours when the selected user's actions on protocols will be logged. Use the right mouse button to mark days and hours when the selected user's actions on protocols will not be logged.*  
**To change audit and shadowing rules for an existing user or group**
    - a. In the upper-left pane of the dialog box, under **Users**, select the user or group.
    - g. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny the appropriate audit and shadowing rights.**To remove an existing user or group and rules**
    - In the upper-left pane of the dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.  
*When you remove a user or group, any rules for that user or group will also be removed.*
6. Click **OK** or **Apply**.

## Enabling offline alerts

Offline alerts for specific access-related events are enabled in the **Auditing, Shadowing & Alerts (Offline)** dialog box. Enabling offline alerts is similar to defining offline audit rules (see [Defining and editing offline audit and shadowing rules](#)) and includes the following basic steps:

- Specify which events will trigger alert notifications. You can enable notification of successful and/or failed attempts to access a protocol. Select the **Alert Allowed** check box to enable notification of successful attempts to access a protocol. Select the **Alert Denied** check box to enable notification of failed attempts to access a protocol.
- Specify users and/or groups whose actions will trigger alert notifications. To do so, in the upper-left pane of the dialog box, under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.

- Specify which user's actions on protocols either will or will not trigger alert notifications. In the upper-left pane of the dialog box, under **Users**, select the user or group that you added. In the lower-left pane of the dialog box, under **User's Rights**, select either **Allow** or **Deny** to directly allow or deny an alert right. Alert rights determine which user actions on protocols trigger alert notifications. Alert rights are identical to audit rights. The only difference is that when events matching specific criteria occur DeviceLock triggers alerts instead of logging these events in the Audit Log. For detailed information on Audit rights for protocols, see [Managing Audit, Shadowing and Alerts for Protocols](#).
- Specify days and hours (for example, from 7 AM to 5 PM Monday through Friday) when the selected user's actions on protocols either will or will not trigger alert notifications. To do so, in the right pane of the dialog box, use the left mouse button to select days and hours when the selected user's actions on protocols will trigger alert notifications. Use the right mouse button to mark days and hours when the selected user's actions on protocols will not trigger alert notifications.

## Undefining offline audit and shadowing rules

You can return previously defined offline audit and shadowing rules to the unconfigured state. If offline rules are undefined, regular rules are applied to offline client computers.

### **To undefine offline audit and shadowing rules**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.  
*When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each protocol in the Offline column.*
4. In the details pane, right-click the protocol for which you want to undefine offline audit and shadowing rules, and then click **Undefine Offline**.  
*You can undefine audit and shadowing rules defined for several protocols at the same time. To do this, do the following:*
  - a. In the details pane, select several protocols by holding down the SHIFT key or the CTRL key while clicking them.



- b. Right-click the selection, and then click **Undefine Offline**.

*The offline state of the audit and shadowing rules changes to "Not Configured."*

## Removing offline audit and shadowing rules

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline audit and shadowing rules and enforce regular audit and shadowing rules on specific lower-level groups of client computers. To enforce regular audit and shadowing rules, offline audit and shadowing rules must be removed.

### **To remove offline audit and shadowing rules**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Auditing, Shadowing & Alerts**.  
*When you select Auditing, Shadowing & Alerts in the console tree, in the details pane you can view protocols for which you can define audit, shadowing rules and alerts. In the details pane you can also view the current state of offline rules for each protocol in the Offline column.*
4. In the details pane, right-click the protocol for which you want to remove offline audit and shadowing rules, and then click **Remove Offline**.  
*You can remove audit and shadowing rules defined for several protocols at the same time. To do this, do the following:*
  - a. In the details pane, select several protocols by holding down the SHIFT key or the CTRL key while clicking them.
  - b. Right-click the selection, and then click **Remove Offline**.  
*The offline state of the audit and shadowing rules changes to "Use Regular."*  
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline Protocols White List

For details on the Protocols White List feature, see [Managing Protocols White List](#).

The offline Protocols White List can have one of the following states:

- **Not Configured** - The white list is not defined. The following message is displayed: "Offline Protocols White List is not configured." This is the default state.
- **Configured** - The white list is defined.
- **Use Regular** - The inheritance of the offline white list is blocked and the regular white list is enforced. The following message is displayed: "Offline Protocols White List is configured to use


Regular Protocols White List.” Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager. The enforcement of the regular white list is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent the offline white list inherited from a higher level from being applied to a specific group of client computers at a lower level. For more information on the enforcement of the regular white list, see [Removing offline Protocols White List](#).

Managing the offline Protocols White List involves the following tasks:

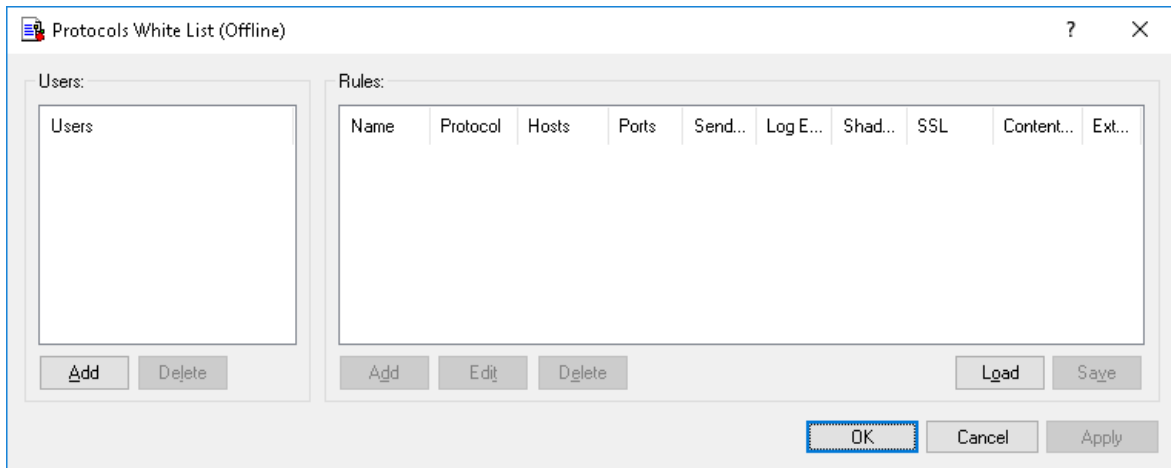
- [Defining offline Protocols White List](#)
- [Editing offline Protocols White List](#)
- [Copying rules of offline Protocols White List](#)
- [Exporting and importing offline Protocols White List](#)
- [Deleting rules of offline Protocols White List](#)
- [Undefined offline Protocols White List](#)
- [Removing offline Protocols White List](#)

## Defining offline Protocols White List

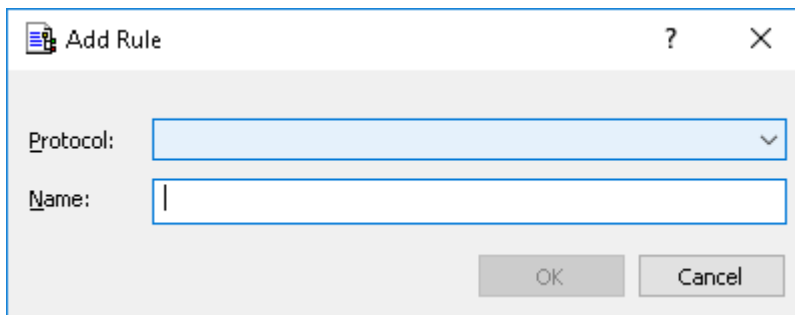
### ***To define the offline Protocols White List***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **White List**, and then click **Manage Offline**.  
- OR -
  - Select **White List**, and then click **Manage Offline**  on the toolbar.

*The Protocols White List (Offline) dialog box appears.*



4. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, click **Add**.  
The *Select Users or Groups dialog box* appears.
5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the Protocols White List, and then click **OK**.  
The users and groups that you added are displayed under **Users** in the left pane of the **Protocols White List (Offline)** dialog box.  
To delete a user or group, in the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete**.
6. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group.  
You can select multiple users or groups by holding down the **SHIFT** key or the **CTRL** key while clicking them.
7. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, click **Add**.  
The *Add Rule dialog box* appears.



8. In the **Add Rule** dialog box, specify general and protocol-specific parameters for this rule. To specify general parameters, do the following:
  - To specify the protocol, in the **Protocol** list, click the protocol of your choice.
  - To specify the rule name, in the **Name** box, type a name.
 To specify protocol-specific parameters, do the following:
  - To enable content inspection, click **Content Inspection**. For more information, see the [Content Inspection](#) parameter description.

- To specify additional actions to be performed when this rule triggers, click **If this rule triggers**. For more information, see the [If this rule triggers](#) parameter description.
- To specify the hosts, in the **Hosts** box, type host names or IP addresses separated by a comma or semicolon. For more information on how to specify hosts, see [Hosts](#) parameter description.
- To specify the ports, in the **Ports** box, type port numbers separated by a comma or semicolon. For more information on how to specify ports, see the [Ports](#) parameter description.
- To specify the Web-based file storage, sharing and synchronization services, under **File Sharing Services**, select the appropriate check boxes. For more information, see the [File Sharing Services](#) parameter description.
- To configure the SSL options, under **SSL**, click any of the following: **Allowed** (allows SSL connections), **Denied** (disallows SSL connections), or **Required** (requires that all connections use SSL).
- To specify the IM local sender ID(s), in the **Local sender ID(s)** box, type user identifiers separated by a comma or semicolon. For more information on how to specify user identifiers, see the [Local sender ID\(s\)](#) parameter description.
- To specify the IM remote recipient ID(s), in the **Remote recipient ID(s)** box, type user identifiers separated by a comma or semicolon. For more information on how to specify user identifiers, see the [Remote recipient ID\(s\)](#) parameter description.
- To specify the e-mail senders, in the **Local sender Email(s)** box, type sender addresses separated by a comma or semicolon. For more information on how to specify sender addresses, see the [Local sender Email\(s\)](#) parameter description.
- To specify the e-mail recipients, in the **Remote recipient Email(s)** box, type recipient addresses separated by a comma or semicolon. For more information on how to specify recipient addresses, see the [Remote recipient Email\(s\)](#) parameter description.
- To specify the social networking sites, under **Social Networks**, select the appropriate check boxes. For more information, see the [Social Networks](#) parameter description.
- To specify the Web-based e-mail services, under **Web Mail Services**, select the appropriate check boxes. For more information, see the [Web Mail Services](#) parameter description.
- To specify the Web search providers, under **Web Search Services**, select the appropriate check boxes. For more information, see the [Web Search Services](#) parameter description.
- To specify the Web-based job search providers, under **Career Search Services**, select the appropriate check boxes. For more information, see the [Career Search Services](#) parameter description.

9. Click **OK**.

*The rule you created is displayed under Rules in the right pane of the Protocols White List (Offline) dialog box.*

10. Click **OK** or **Apply**.

*The users or groups to which the white list rule applies are displayed under White List in the console tree.*

When you select a user or group to which a white list rule applies in the console tree, in the details pane you can view detailed information regarding this rule (see [White List Rules](#)).

You can define different online vs. offline Protocols White Lists for the same user or sets of users. For information about how to define the online Protocols White List, see [Managing Protocols White List](#).

## Editing offline Protocols White List

You can modify parameter values specified for an offline white list rule any time you want.


### **To edit an offline white list rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, click **Manage Offline**, and then do the following:
  - a. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the white list rules applied to them under Rules in the right pane of the dialog box.*
  - b. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.  
- OR -  
Right-click the rule, and then click **Edit**.  
- OR -  
Under **Protocols**, expand **White List**, and then do the following:
    - a. Under **White List**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the white list rules applied to them in the details pane.*
  - c. In the details pane, right-click the rule you want to edit, and then click **Edit**.  
- OR -  
In the details pane, double-click the rule you want to edit.  
*The Edit Rule dialog box appears.*
4. In the **Edit Rule** dialog box, modify the rule parameters as required to meet your needs.
5. Click **OK** to apply the changes.

## Copying rules of offline Protocols White List

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing rules of the offline Protocols White List.

### **To copy an offline white list rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **White List**, and then click **Manage Offline**.
  - OR -
  - Select **White List**, and then click **Manage Offline**  on the toolbar.



*The Protocols White List (Offline) dialog box appears.*
4. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.  
*By selecting users or groups, you can view the white list rules applied to them under Rules in the right pane of the dialog box.*
5. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.  
*The rule you cut or copy is automatically copied to the Clipboard.*  
*You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.*
6. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, click **Add**.
7. In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.  
*The users and groups that you added are displayed under Users in the left pane of the Protocols White List (Offline) dialog box.*
8. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*

9. In the right pane of the **Protocols White List (Offline)** dialog box, right-click in the **Rules** pane and then click **Paste**.  
*The copied rule is displayed under Rules in the right pane of the Protocols White List dialog box.*
10. Click **OK** or **Apply** to apply the copied rule.



## Exporting and importing offline Protocols White List

You can export all your current rules of the offline Protocols White List to a .pwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

### **To export the offline Protocols White List**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **White List**, and then click **Save Offline**.  
 - OR -
  - Select **White List**, and then click **Save Offline**  on the toolbar.  
 - OR -
  - Expand **White List**, right-click any user or group specified in the white list, and then click **Save Offline**.  
 - OR -
  - Expand **White List**, select any user or group specified in the white list. In the details pane, right-click the white list rule, and then click **Save**.  
 - OR -
  - Expand **White List**, select any user or group specified in the white list, and then click **Save Offline**  on the toolbar.  
 - OR -
  - Right-click **White List**, and then click **Manage Offline**. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, click **Save**.
4. In the **Save As** dialog box that appears, choose the folder where you want to save the .pwl file, specify the file name, and then click **Save**.  
*When you export the offline Protocols White List, it is saved in a file with a .pwl extension.*

### **To import the offline Protocols White List**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **White List**, and then click **Load Offline**.  
- OR -
  - Select **White List**, and then click **Load Offline**  on the toolbar.  
- OR -
  - Expand **White List**, right-click any user or group specified in the white list, and then click **Load Offline**.  
- OR -
  - Expand **White List**, select any user or group specified in the white list. In the details pane, right-click the white list rule, and then click **Load**.  
- OR -
  - Expand **White List**, select any user or group specified in the white list, and then click **Load Offline**  on the toolbar.  
- OR -
  - Right-click **White List**, and then click **Manage Offline**. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, click **Load**.
4. In the **Open** dialog box that appears, locate and select the file you want to import, and then click **Open**.  
*If the offline Protocols White List is already defined and you choose to import a new offline white list, the following message is displayed: "Do you want to overwrite existing records (Yes - Overwrite, No - Append)?" In the message box, click Yes to overwrite the existing offline white list. Click No to append a new offline white list to the existing offline white list.*

## Deleting rules of offline Protocols White List

You can delete individual rules of the offline Protocols White List when they are no longer required.

### **To delete an offline white list rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.



- b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
  3. Under **Protocols**, do one of the following:
    - Expand **White List**, right-click the user or group to which the rule is applied, and then click **Delete user**.  
*When you delete a user or group, the rule associated with this user or group is automatically deleted.*  
- OR -
    - Expand **White List**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.  
- OR -
    - Right-click **White List**, and then click **Manage Offline**. In the left pane of the **Protocols White List (Offline)** dialog box, under **Users**, select the user or group to which the rule is applied. In the right pane of the **Protocols White List (Offline)** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

## Undefining offline Protocols White List

You can return the previously defined offline white list to the unconfigured state. If the offline white list is undefined, the regular white list is applied to offline client computers.

### ***To undefine the offline Protocols White List***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, and then click **Undefine Offline**.  
*The offline state of the white list changes to "Not Configured."*  
When you select **White List** in the console tree, in the details pane the following message is displayed: "Offline Protocols White List is not configured."

## Removing offline Protocols White List

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of the higher-level offline white list and enforce the regular white list on specific lower-level groups of client computers. To enforce the regular Protocols White List, the offline Protocols White List must be removed.

### **To remove the offline Protocols White List**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **White List**, and then click **Remove Offline**.

*The offline state of the white list changes to "Use Regular."*

When you select **White List** in the console tree, in the details pane the following message is displayed: "Offline Protocols White List is configured to use Regular Protocols White List."

*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline IP Firewall

For details on the Basic IP Firewall feature, see [Managing Basic IP Firewall](#).

The offline IP Firewall can have one of the following states:

- **Not Configured** - The IP Firewall is not configured. The following message is displayed: "Offline Basic IP Firewall is not configured." This is the default state.
- **Configured** - The IP Firewall is configured.
- **Use Regular** - The inheritance of the offline IP Firewall is blocked and the regular IP Firewall is enforced. The following message is displayed: "Offline Basic IP Firewall is configured to use Regular Basic IP Firewall." Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.

The enforcement of the regular IP Firewall is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent the offline IP Firewall inherited from a higher level from being applied to a specific group of client computers at a lower level.

For more information on the enforcement of the regular IP Firewall, see [Removing offline firewall rules](#).

Managing offline firewall rules involves the following tasks:


- [Defining offline firewall rules](#)
- [Editing offline firewall rules](#)
- [Copying offline firewall rules](#)
- [Exporting and importing offline firewall rules](#)
- [Deleting offline firewall rules](#)
- [Undefining offline firewall rules](#)
- [Removing offline firewall rules](#)

## Defining offline firewall rules

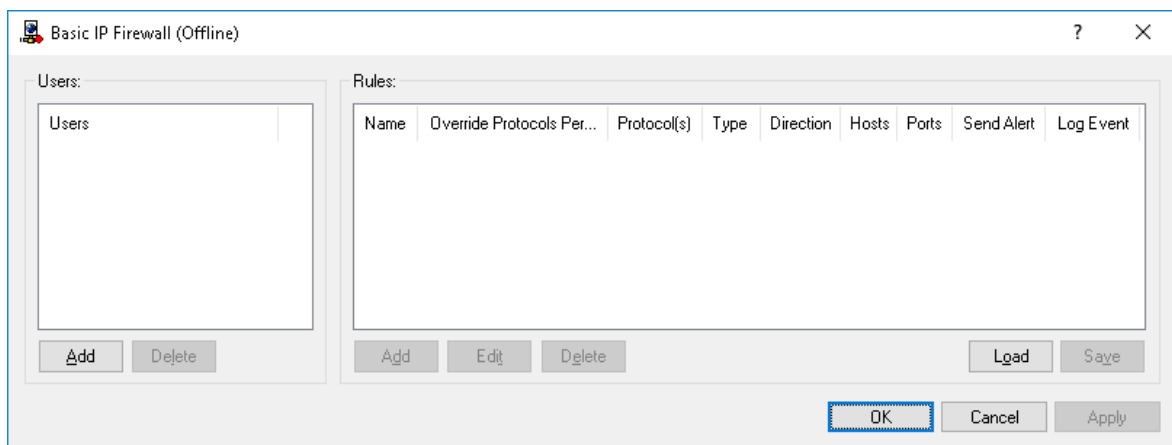
You can enable offline alerts that are sent when a specific offline firewall rule fires. Such alerts are enabled immediately after setting up an offline firewall rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific firewall rule, alert settings must be configured in DeviceLock Service options (see [Alerts](#)).

### ***To define an offline firewall rule***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Basic IP Firewall**, and then click **Manage Offline**.  
- OR -
  - Select **Basic IP Firewall**, and then click **Manage Offline**  on the toolbar.

*The Basic IP Firewall (Offline) dialog box appears.*



4. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, click **Add**.  
*The **Select Users or Groups** dialog box appears.*
5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the firewall rule, and then click **OK**.  
*The users and groups that you added are displayed under **Users** in the left pane of the **Basic IP Firewall (Offline)** dialog box.*  
 To delete a user or group, in the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete**.
6. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group.  
*You can select multiple users or groups by holding down the **SHIFT** key or the **CTRL** key while clicking them.*
7. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, click **Add**.  
*The **Add Rule** dialog box appears.*
8. In the **Add Rule** dialog box, specify the firewall rule parameters:
  - To specify the rule name, in the **Name** box, type a name.
  - To block access to the hosts specified by the **Hosts** setting, select the **Override Protocols Permissions** check box. For more information, see the [Override Protocols Permissions](#) parameter description.
  - To specify the protocol, under **Protocol**, select the check box next to the protocol of your choice. For more information, see the [Protocol](#) parameter description.
  - To specify what actions the firewall takes for all connections that match the rule's criteria, under **Type**, click either of the following options: **Allow** or **Deny**. For more information, see the [Type](#) parameter description.
  - To specify the direction of traffic to which the rule applies, under **Direction**, select the appropriate check box. For more information, see the [Direction](#) parameter description.
  - To specify additional actions to be performed when the rule triggers, under **If this rule triggers**, select the appropriate check box. For more information, see the [If this rule triggers](#) parameter description.

- To specify the remote hosts to which the rule applies, in the **Hosts** box, type host names or IP addresses separated by a comma or semicolon. For more information, see the [Hosts](#) parameter description.
- To specify the ports on remote hosts to which the rule applies, in the **Ports** box, type port numbers separated by a comma or semicolon. For more information, see the [Ports](#) parameter description.

9. Click **OK**.

*The rule you created is displayed under Rules in the right pane of the Basic IP Firewall (Offline) dialog box.*

10. Click **OK** or **Apply**.

*The users or groups to which the firewall rule applies are displayed under Basic IP Firewall in the console tree.*

When you select a user or group to which a firewall rule applies in the console tree, in the details pane you can view detailed information regarding this rule (see [Firewall Rules](#)).

You can define different online vs. offline firewall rules for the same user or sets of users. For information about how to define online firewall rules, see [Managing Basic IP Firewall](#).

## Editing offline firewall rules

You can modify parameter values specified for an offline firewall rule any time you want.

### **To edit an offline firewall rule**


1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file with defined offline DeviceLock policies.
  - d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, click **Manage Offline**, and then do the following:
  - a. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the firewall rules applied to them under Rules in the right pane of the dialog box.*

- b. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.
  - OR -
  - Right-click the rule, and then click **Edit**.
  - OR -
  - Under **Protocols**, expand **Basic IP Firewall**, and then do the following:
    - a. Under **Basic IP Firewall**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the firewall rules applied to them in the details pane.*
- c. In the details pane, right-click the rule you want to edit, and then click **Edit**.
  - OR -
  - In the details pane, double-click the rule you want to edit.  
*The Edit Rule dialog box appears.*
4. In the **Edit Rule** dialog box, modify the rule parameters as required to meet your needs.
5. Click **OK** to apply the changes.

## Copying offline firewall rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing offline firewall rules.

### **To copy an offline firewall rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file with defined offline DeviceLock policies.
  - d. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Basic IP Firewall**, and then click **Manage Offline**.
  - OR -
  - Select **Basic IP Firewall**, and then click **Manage Offline**  on the toolbar.
4. In the left pane of the **Basic IP Firewall (Offline)** dialog box that appears, under **Users**, select the user or group to which the rule that you want to copy is applied.

*By selecting users or groups, you can view the firewall rules applied to them under Rules in the right pane of the dialog box.*

5. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

*The rule you cut or copy is automatically copied to the Clipboard.*

*You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.*

*You can copy and then paste several rules at the same time. Hold down the SHIFT key or the CTRL key while you click each rule, right-click one of them, and then click **Copy**.*

6. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, click **Add**.

*The Select Users or Groups dialog box appears.*

7. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

*The users and groups that you added are displayed under Users in the left pane of the Basic IP Firewall (Offline) dialog box.*

8. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*

9. In the right pane of the **Basic IP Firewall (Offline)** dialog box, right-click in the **Rules** pane and then click **Paste**.

*The copied rule is displayed under Rules in the right pane of the Basic IP Firewall (Offline) dialog box.*



10. Click **OK** or **Apply** to apply the copied rule.

## Exporting and importing offline firewall rules


You can export all your current offline firewall rules to an .ipp file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.

### **To export offline firewall rules**


1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file with defined offline DeviceLock policies.
  - d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.

2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Basic IP Firewall**, and then click **Save Offline**.  
- OR -
  - Select **Basic IP Firewall**, and then click **Save Offline**  on the toolbar.  
- OR -
  - Expand **Basic IP Firewall**, right-click any user or group specified in the firewall rule, and then click **Save Offline**.  
- OR -
  - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule. In the details pane, right-click the firewall rule, and then click **Save**.  
- OR -
  - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule, and then click **Save Offline**  on the toolbar.  
- OR -
  - Right-click **Basic IP Firewall**, and then click **Manage Offline**. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, click **Save**.
4. In the **Save As** dialog box that appears, choose the folder where you want to save the .ipp file, specify the file name, and then click **Save**.  
*When you export offline firewall rules, they are saved in a file with an .ipp extension.*

### ***To import offline firewall rules***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Basic IP Firewall**, and then click **Load Offline**.  
- OR -
  - Select **Basic IP Firewall**, and then click **Load Offline**  on the toolbar.  
- OR -
  - Expand **Basic IP Firewall**, right-click any user or group specified in the firewall rule, and then click **Load Offline**.  
- OR -



- Expand **Basic IP Firewall**, select any user or group specified in the firewall rule. In the details pane, right-click the firewall rule, and then click **Load**.  
- OR -
  - Expand **Basic IP Firewall**, select any user or group specified in the firewall rule, and then click **Load Offline**  on the toolbar.  
- OR -
  - Right-click **Basic IP Firewall**, and then click **Manage Offline**. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, click **Load**.
4. In the **Open** dialog box that appears, locate and select the file you want to import, and then click **Open**.
- If offline firewall rules are already defined and you choose to import new offline firewall rules, the following message is displayed: "Do you want to overwrite existing records (Yes - Overwrite, No - Append)?" In the message box, click Yes to overwrite the existing offline firewall rules. Click No to append new offline firewall rules to the existing offline firewall rules.*

## Deleting offline firewall rules

You can delete individual offline firewall rules when they are no longer required.

### **To delete an offline firewall rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file with defined offline DeviceLock policies.
  - d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Expand **Basic IP Firewall**, right-click the user or group to which the rule is applied, and then click **Delete user**.  
*When you delete a user or group, the rule associated with this user or group is automatically deleted.*  
- OR -
  - Expand **Basic IP Firewall**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.  
- OR -

- Right-click **Basic IP Firewall**, and then click **Manage Offline**. In the left pane of the **Basic IP Firewall (Offline)** dialog box, under **Users**, select the user or group to which the rule is applied. In the right pane of the **Basic IP Firewall (Offline)** dialog box, under **Rules**, select the rule, and then click **Delete** or right-click the rule, and then click **Delete**.

## Undefining offline firewall rules

You can return the previously defined offline firewall rules to the unconfigured state. If offline firewall rules are undefined, regular firewall rules are applied to offline client computers.

### ***To undefine offline firewall rules***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file with defined offline DeviceLock policies.
  - d. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - e. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Undefine Offline**.  
*The offline state of the IP Firewall changes to "Not Configured."*  
When you select **Basic IP Firewall** in the console tree, in the details pane the following message is displayed: "Offline Basic IP Firewall is not configured."

## Removing offline firewall rules

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline firewall rules and enforce regular firewall rules on specific lower-level groups of client computers. To enforce regular firewall rules, offline firewall rules must be removed.

### ***To remove offline firewall rules***

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.

- c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Remove Offline**.  
*The offline state of the IP Firewall changes to "Use Regular."*  
When you select **Basic IP Firewall** in the console tree, in the details pane the following message is displayed: "Offline Basic IP Firewall is configured to use Regular Basic IP Firewall."  
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*

## Managing Offline Content-Aware Rules for Protocols

For details on the Content-Aware Rules feature for protocols, see [Rules for Protocols](#) in [Content-Aware Rules \(Regular Profile\)](#).

The offline Content-Aware Rules can have one of the following states:

- **Not Configured** - Content-Aware Rules are not defined. The following message is displayed: "Offline Content-Aware Rules are not configured." This is the default state.
- **Configured** - Content-Aware Rules are defined.
- **Use Regular** - The inheritance of offline Content-Aware Rules is blocked and regular Content-Aware Rules are enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.  
The enforcement of regular Content-Aware Rules is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent offline Content-Aware Rules inherited from a higher level from being applied to a specific group of client computers at a lower level.  
For more information on the enforcement of regular Content-Aware Rules, see [Removing offline Content-Aware Rules](#).

Managing offline Content-Aware Rules involves the following tasks:

- [Defining offline Content-Aware Rules](#)
- [Editing offline Content-Aware Rules](#)
- [Copying offline Content-Aware Rules](#)
- [Exporting and importing offline Content-Aware Rules](#)
- [Deleting offline Content-Aware Rules](#)
- [Undefining offline Content-Aware Rules](#)
- [Removing offline Content-Aware Rules](#)


## Defining offline Content-Aware Rules

Content-Aware Rules are created based on either the built-in or custom content groups. For detailed information on these groups, see [Configuring Content Groups](#).

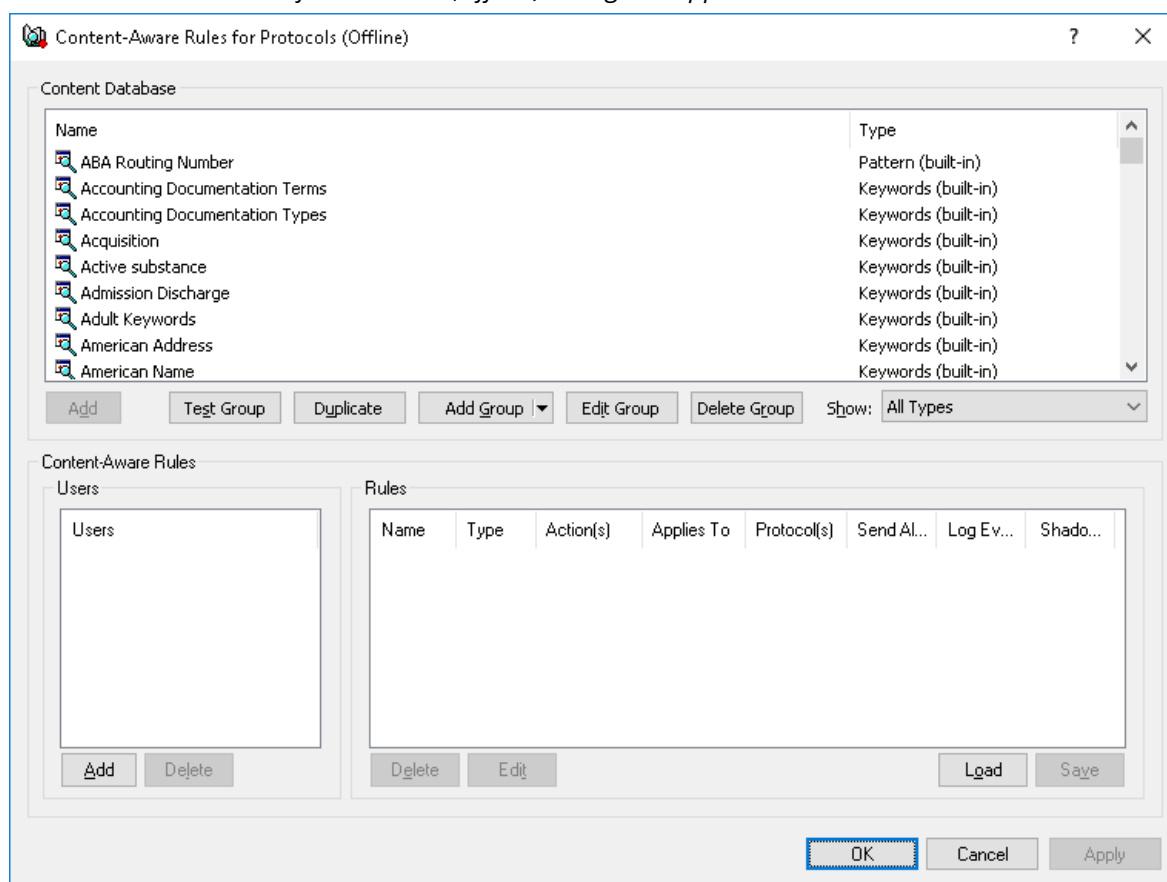
You can enable offline alerts that are sent when a specific offline Content-Aware Rule fires. Such alerts are enabled immediately after setting up an offline Content-Aware Rule.

DeviceLock sends alerts on the basis of alert settings. These settings specify where and how the alerts should be sent. Before enabling alerts for a specific Content-Aware Rule, alert settings must be configured in DeviceLock Service options (see [Alerts](#)).

### ***To define an offline Content-Aware Rule***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage Offline**.
  - OR -
  - Select **Content-Aware Rules**, and then click **Manage Offline**  on the toolbar.

*The Content-Aware Rules for Protocols (Offline) dialog box appears.*



4. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, click **Add**.  
*The Select Users or Groups dialog box appears.*
5. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the names of the users or groups for which you want to define the rule, and then click **OK**.  
*The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Protocols (Offline) dialog box.*  
To delete a user or group, in the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the user or group, and then click **Delete** or press the DELETE key.
6. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the users or groups for which you want to define the rule.  
*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*
7. In the upper pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Content Database**, select the desired content group, and then click **Add**, or double-click the desired content group.

---

**Note**

You can specify only one content group for a Content-Aware Rule.

---

*The Add Rule dialog box appears.*

**Add Rule**

Name:

Applies to: ☐ Permissions ☐ Shadowing ☐ Detection

If this rule triggers: ☐ Send Alert ☐ Log Event ☐ Shadow Copy

Protocol(s):

Actions

	Allow	Deny
User's Rights		

View Group OK Cancel

8. In the **Add Rule** dialog box, in the **Name** box, type the name of the Content-Aware Rule. By default, the rule has the same name as its content group. The name of the rule can be changed if needed.  
To view this rule's content group, click the **View Group** button in the bottom left corner of the dialog box. The console displays the properties of the group in a separate dialog box, allowing property values to be viewed but not modified.
9. Under **Applies to**, specify the type of operation associated with the rule. The available options are:
  - **Permissions** - Specifies that the rule will apply to access control operations.
  - **Shadowing** - Specifies that the rule will apply to shadow copy operations.
  - **Detection** - Specifies that the rule will apply to detection operations.
  - **Permissions, Shadowing** - Specifies that the rule will apply to both access control and shadow copy operations.
  - **Permissions, Detection** - Specifies that the rule will apply to both access control and detection operations.

- **Shadowing, Detection** - Specifies that the rule will apply to both shadow copy and detection operations.
- **Permissions, Shadowing, Detection** - Specifies that the rule will apply to all available operations: access control, shadow copy, and detection.

---

#### Note

To successfully create/save a rule that applies either to detection operations only or to detection operations combined with other operations, at least one of the following options must be selected for this rule: **Log Event**, **Send Alert** or **Shadow Copy** (see step 10 of this procedure). Otherwise, the rule cannot be saved and the following message appears: "Log Event, Send Alert or Shadow Copy should be specified."

---

- Under **If this rule triggers**, specify the following additional actions to be performed when the rule triggers:

- **Send Alert** - Specifies that an alert is sent whenever the rule triggers.
- **Log Event** - Specifies that an event is logged in the Audit Log whenever the rule triggers.
- **Shadow Copy** - Specifies that a shadow copy of data is created whenever the rule triggers.

When alerts, audit and/or shadowing are enabled or disabled in a Content-Aware Rule, the rule setting takes precedence over the respective setting for the protocol.

Example: If audit is enabled for a particular protocol and disabled in a rule for that protocol, the triggering of the rule does not cause audit events. If audit is enabled in the rule, then the triggering of the rule causes audit events, even if audit is disabled at the protocol level.

The rule can also inherit the alert, audit and/or shadowing setting from the protocol level. This is the default option, represented by the indeterminate state of the check boxes (neither checked nor cleared). The state of each check box can be changed individually.

Example: When a rule inherits the audit setting from the protocol level, the triggering of the rule causes audit events only if audit is enabled for the protocol controlled by that rule.

- Under **Protocol(s)**, select the appropriate protocol(s) you would like this rule to be applied to. *Content-Aware Rules can be applied to the following protocols: Career Search, File Sharing, FTP, HTTP, IBM Notes, ICQ Messenger, IRC, Jabber, Mail.Ru Agent, MAPI, Skype, SMB, SMTP, Social Networks, Telegram, Viber, Web Mail, Web Search, WharsApp, and Zoom.*

*Under Action(s), if you multi-select protocols that have different combinations of configurable access rights, the dialog box will display the superset of access rights for the selection list: those that are common to all selected protocols, and those that do not necessarily apply to all protocols. As would be expected, if a particular access right that is displayed is not common to one or more particular selected protocols, it's setting will not/cannot be applied to those protocols and will only apply to protocols where the setting is supported.*

- Under **Action(s)**, specify which user actions are allowed or disallowed on protocols, which user actions are logged to the Shadow Log, and which user actions are detected.  
If the rule applies to shadow copy operations combined with other operations, the Read user right becomes unavailable. If the rule applies to detection operations combined with other operations, only Allow action becomes available. For detailed information on user rights and

actions that can be specified in Content-Aware Rules, see [Access Control](#), [Content-Aware Shadowing](#) and [Content-Aware Detection](#) for protocols.

13. Click **OK**.

*The rule you created is displayed under Rules in the lower-right pane of the Content-Aware Rules for Protocols (Offline) dialog box.*

14. Click **OK** or **Apply** to apply the rule.

*The users or groups to which the Content-Aware Rule applies are displayed under Content-Aware Rules in the console tree.*

When you select a user or group to which a Content-Aware Rule applies in the console tree, in the details pane you can view detailed information regarding this rule (see [List of Content-Aware Rules for Protocols](#)).

You can define different online vs. offline Content-Aware Rules for the same user or sets of users. For information about how to define online Content-Aware Rules for protocols, see [Managing Content-Aware Rules](#).

## Editing offline Content-Aware Rules

You can modify the Content-Aware Rule properties such as **Name**, **Applies To**, **If this rule triggers**, **Protocol(s)**, **Actions**.

### **To edit an offline Content-Aware Rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Content-Aware Rules**, click **Manage Offline**, and then do the following:
  - a. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.*
  - b. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, select the rule you want to edit, and then click **Edit**.  
- OR -  
Right-click the rule, and then click **Edit**.



- OR -

Double-click the rule.

- OR -

Under **Protocols**, expand **Content-Aware Rules**, and then do the following:

- a. Under **Content-Aware Rules**, select the user or group for which you want to edit the rule.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them in the details pane.*

- c. In the details pane, right-click the rule you want to edit, and then click **Edit**.

- OR -

In the details pane, double-click the rule you want to edit.


*The Edit Rule dialog box appears.*

4. In the **Edit Rule** dialog box, modify the rule properties as required to meet your needs.
5. Click **OK** to apply the changes.

## Copying offline Content-Aware Rules

You can perform a cut-and-paste operation, a copy-and-paste operation or a drag-and-drop operation to reuse existing offline Content-Aware Rules.

### To copy an offline Content-Aware Rule

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Manage Offline**.
  - OR -
  - Select **Content-Aware Rules**, and then click **Manage Offline**  on the toolbar.

*The Content-Aware Rules for Protocols (Offline) dialog box appears.*
4. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the user or group to which the rule that you want to copy is applied.  
*By selecting users or groups, you can view the Content-Aware Rules applied to them under Rules in the lower-right pane of the dialog box.*
5. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, right-click the rule you want to copy, and then click **Copy** or **Cut**.

*The rule you cut or copy is automatically copied to the Clipboard.*

*You can use the CTRL+C, CTRL+X and CTRL+V key combinations to copy, cut and paste the rule. When you use the CTRL+X key combination to cut the rule, the rule will be cut only after you paste it.*

To perform a drag-and-drop operation, select the rule and move it to the user or group to which you want to apply the copied rule.

6. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, click **Add**.

7. In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the names of the users or groups to which you want to apply the copied rule, and then click **OK**.

*The users and groups that you added are displayed under Users in the lower-left pane of the Content-Aware Rules for Protocols (Offline) dialog box.*

8. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the users or groups to which you want to apply the copied rule.

*You can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.*

9. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, right-click in the **Rules** pane and then click **Paste**.

*The copied rule is displayed under Rules in the lower-right pane of the Content-Aware Rules for Protocols (Offline) dialog box.*



10. Click **OK** or **Apply** to apply the copied rule.

## Exporting and importing offline Content-Aware Rules


You can export all your current offline Content-Aware Rules to a .cwl file that you can import and use on another computer. Exporting and importing can also be used as a form of backup.


### **To export offline Content-Aware Rules**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Save Offline**.
  - OR -

- Select **Content-Aware Rules**, and then click **Save Offline**  on the toolbar.
    - OR -
  - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Save Offline**.
    - OR -
  - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Save**.
    - OR -
  - Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Save Offline**  on the toolbar.
    - OR -
  - Right-click **Content-Aware Rules**, and then click **Manage Offline**. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, click **Save**.
4. In the **Save As** dialog box that appears, choose the folder where you want to save the .cwl file, specify the file name, and then click **Save**.
- When you export rules, they are saved in a file with a .cwl extension.*

### **To import offline Content-Aware Rules**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Right-click **Content-Aware Rules**, and then click **Load Offline**.
    - OR -
  - Select **Content-Aware Rules**, and then click **Load Offline**  on the toolbar.
    - OR -
  - Expand **Content-Aware Rules**, right-click any user or group to which the rule is applied, and then click **Load Offline**.
    - OR -
  - Expand **Content-Aware Rules**, and then select any user or group to which the rule is applied. In the details pane, right-click the rule, and then click **Load**.
    - OR -

- Expand **Content-Aware Rules**, select any user or group to which the rule is applied, and then click **Load Offline**  on the toolbar.
  - OR -
  - Right-click **Content-Aware Rules**, and then click **Manage Offline**. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, click **Load**.
4. In the **Open** dialog box that appears, locate and select the file to import, and then click **Open**.  
*You can import only one .cwl file at a time.*

## Deleting offline Content-Aware Rules

You can delete individual offline Content-Aware Rules when they are no longer required.

### **To delete an offline Content-Aware Rule**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
 If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Expand **Content-Aware Rules**, right-click the user or group to which the rule is applied, and then click **Delete user**.  
*When you delete a user or group, the rule associated with this user or group is automatically deleted.*
  - OR -
  - Expand **Content-Aware Rules**, and then select the user or group to which the rule is applied. In the details pane, right-click the rule associated with this user or group, and then click **Delete**.
  - OR -
  - Right-click **Content-Aware Rules**, and then click **Manage Offline**. In the lower-left pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Users**, select the user or group to which the rule is applied. In the lower-right pane of the **Content-Aware Rules for Protocols (Offline)** dialog box, under **Rules**, select the rule, and then click **Delete**.  
*You can select multiple rules that you want to delete by holding down the SHIFT key or the CTRL key while clicking them.*

## Undefining offline Content-Aware Rules

You can return the previously defined offline Content-Aware Rules to the unconfigured state. If offline rules are undefined, regular rules are applied to offline client computers.

### **To undefine offline Content-Aware Rules**

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Content-Aware Rules**, and then click **Undefine Offline**.  
*The offline state of Content-Aware Rules changes to "Not Configured."*  
When you select **Content-Aware Rules** in the console tree, in the details pane the following message is displayed: "Offline Content-Aware Rules are not configured."

## Removing offline Content-Aware Rules

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline Content-Aware Rules and enforce regular Content-Aware Rules on specific lower-level groups of client computers. To enforce regular Content-Aware Rules, offline Content-Aware Rules must be removed.

### **To remove offline Content-Aware Rules**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - c. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, right-click **Content-Aware Rules**, and then click **Remove Offline**.  
*The offline state of Content-Aware Rules changes to "Use Regular."*  
When you select **Content-Aware Rules** in the console tree, in the details pane the following message is displayed: "Offline Content-Aware Rules are configured to use Regular Content-Aware Rules."

*The “Use Regular” state of DeviceLock Service settings is displayed as “Not Configured” in DeviceLock Management Console.*

## Managing Offline Security Settings for Protocols

For details on the Security Settings feature for protocols, see [Managing Security Settings for Protocols](#).

Offline Security Settings can have one of the following states:

- **Not Configured** - Security Settings are not defined for protocols. This is the default state.
- **Enabled** - Security Settings are enabled for protocols.
- **Disabled** - Security Settings are disabled for protocols.
- **Use Regular** - The inheritance of offline Security Settings is blocked and regular Security Settings are enforced. Offline DeviceLock Service settings can have this state only in DeviceLock Service Settings Editor or DeviceLock Group Policy Manager.

The enforcement of regular Security Settings is helpful when using Group Policy or DeviceLock Service settings files (.dls) to deploy DeviceLock policies throughout the network as this kind of enforcement can be used to prevent offline Security Settings inherited from a higher level from being applied to a specific group of client computers at a lower level.

For more information on the enforcement of regular Security Settings, see [Removing offline Security Settings](#).


Managing offline Security Settings involves the following tasks:

- [Defining and changing offline Security Settings](#)
- [Undefining offline Security Settings](#)
- [Removing offline Security Settings](#)

## Defining and changing offline Security Settings

### ***To define and change offline Security Settings***

1. If using DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.

3. Under **Protocols**, do one of the following:
  - Select **Security Settings**. In the details pane, right-click the **Security Setting**, and then click **Enable Offline** or **Disable Offline**.  
*When you select Security Settings in the console tree, they are displayed in the details pane.*
  - OR -
  - Right-click **Security Settings**, and then click **Manage Offline**. In the **Security Settings (Offline)** dialog box that opens, select or clear the appropriate check box, and then click **OK**.  
*To open the Security Settings (Offline) dialog box, you can also select Security Settings, and then click Manage Offline  on the toolbar.*

---

#### Note

All check boxes in the **Security Settings (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of Security Settings.


---

*The Security Setting changes its offline state from "Not Configured" to "Enabled" or "Disabled."*

## Undefining offline Security Settings

You can return the previously defined offline Security Settings to the unconfigured state. If offline Security Settings are undefined, regular Security Settings are applied to offline client computers.

### **To undefine offline Security Settings**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file with defined offline DeviceLock policies.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, do one of the following:
  - Select **Security Settings**. In the details pane, right-click the Security Setting, and then click **Undefine Offline**.  
*When you select Security Settings in the console tree, they are displayed in the details pane.*
  - OR -
  - Right-click **Security Settings**, and then click **Manage Offline**. In the **Security Settings (Offline)** dialog box that opens, return the appropriate check box to the indeterminate state, and then click **OK**.  
*To open the Security Settings (Offline) dialog box, you can also select Security Settings, and then click Manage Offline  on the toolbar.*

---

**Note**

All check boxes in the **Security Settings (Offline)** dialog box have three states: selected, cleared, and indeterminate that correspond to the Enabled, Disabled, and Not Configured states of Security Settings.

---

*The Security Setting changes its offline state to "Not Configured."*

## Removing offline Security Settings

To facilitate deployment of DeviceLock policies using Group Policy or DeviceLock Service settings files (.dls), DeviceLock provides the ability to block the inheritance of higher-level offline Security Settings and enforce regular Security Settings on specific lower-level groups of client computers. To enforce regular Security Settings, offline Security Settings must be removed. The console allows you to remove only individual Security Settings one by one.

### **To remove offline Security Settings**

1. If using DeviceLock Service Settings Editor, do the following:
  - a. Open DeviceLock Service Settings Editor.
  - b. In the console tree, right-click **DeviceLock Settings** or **DeviceLock Service**, and then click **Load Service Settings** to open the DeviceLock Service settings file with defined offline DeviceLock policies.
  - c. In the console tree, expand **DeviceLock Service**.  
If using DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Expand **Protocols**.
3. Under **Protocols**, select **Security Settings**.  
*When you select Security Settings in the console tree, they are displayed in the details pane.*
4. In the details pane, right-click the Security Setting to remove, and then click **Remove Offline**.

*The Security Setting changes its offline state to "Use Regular."*

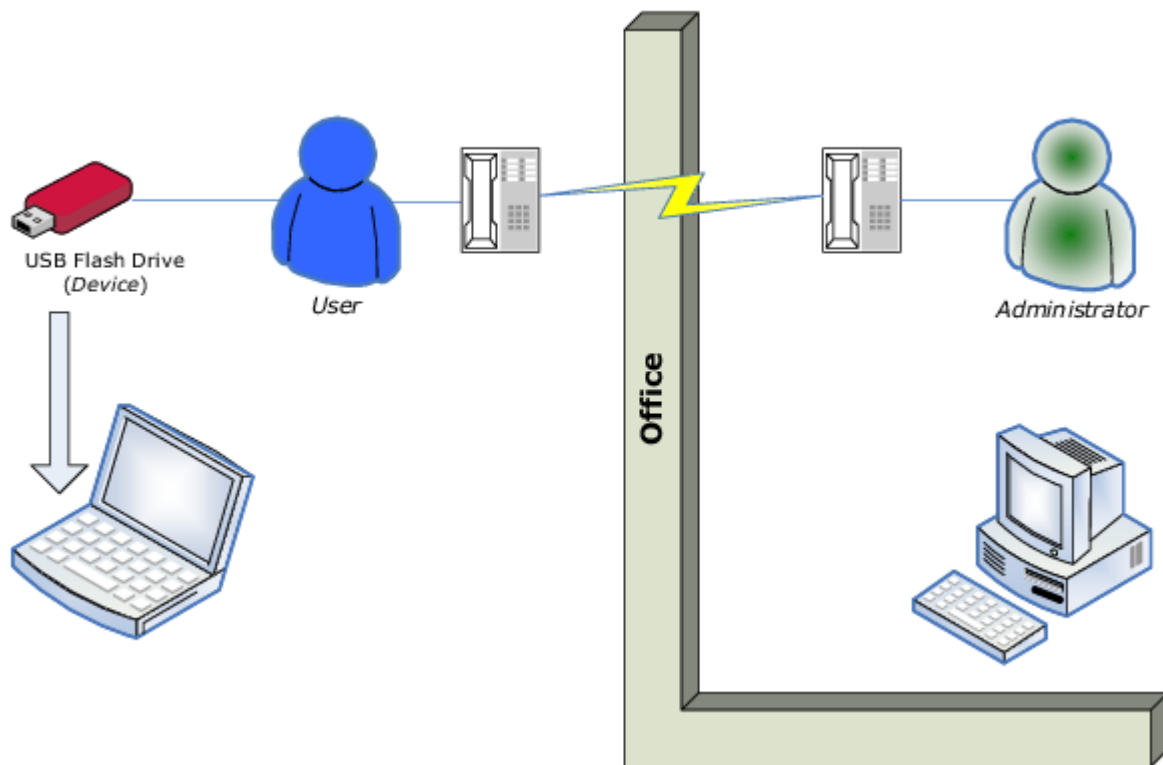
*The "Use Regular" state of DeviceLock Service settings is displayed as "Not Configured" in DeviceLock Management Console.*



# Temporary White List

## Overview

The DeviceLock Temporary White List function enables the granting of temporary access to USB devices when there is no network connection. Administrators provide users with special access codes over the phone that temporarily unlock access to requested devices. The following diagram illustrates the process of granting temporary access to USB devices.



A Temporary White List works like a device white list (see [USB Devices White List \(Regular Profile\)](#)), with the distinction that a network connection is not required to add devices and grant access to them.

---

### Note

Using Temporary White List it is possible to grant access to USB devices that were blocked on both levels: the USB port level and the type level. If some white listed device (for example, USB Flash Drive) belongs to both levels: USB and type (Removable), the permissions (if any) for the type level are ignored as well as for the USB level.

---

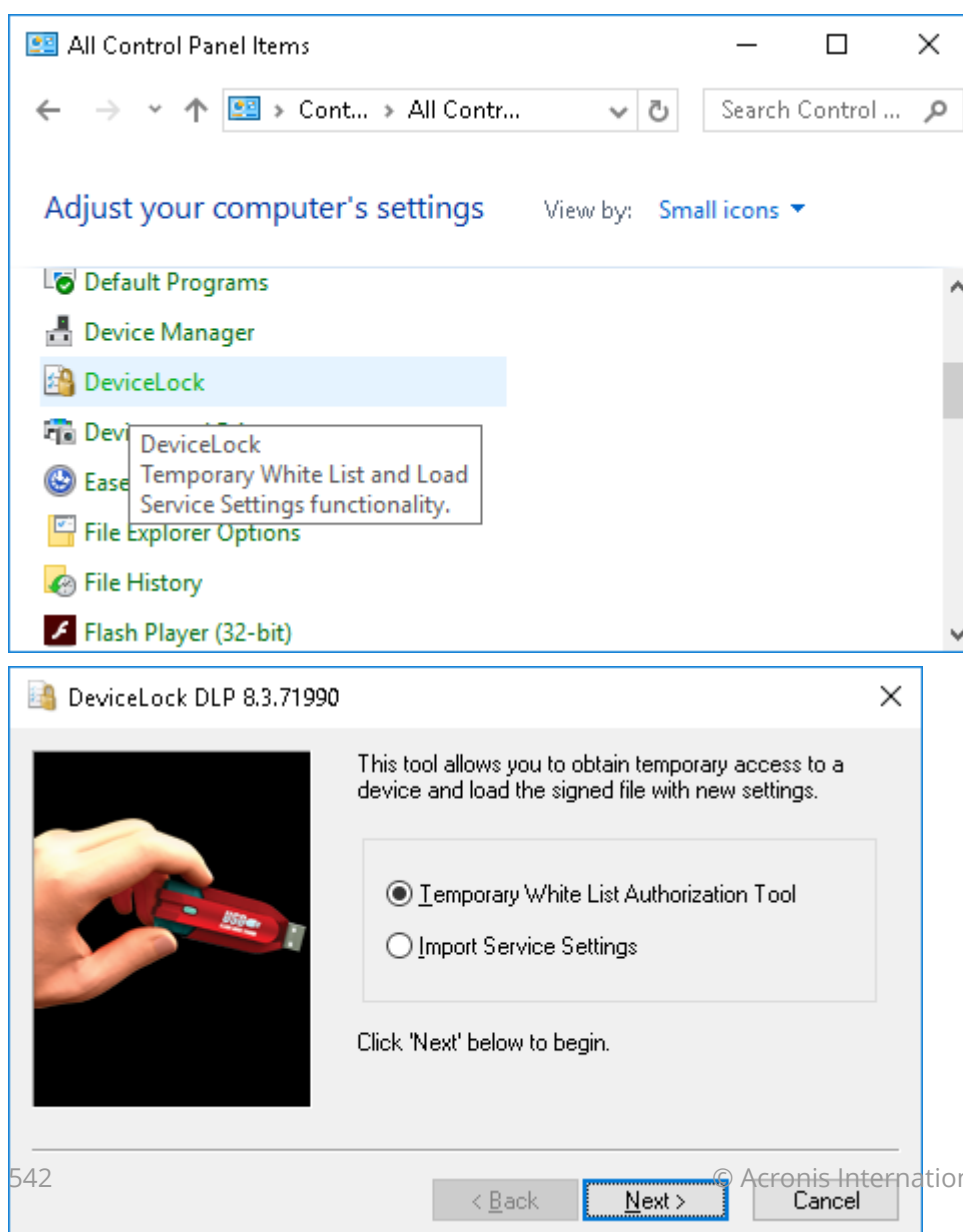
Creating and activating a Temporary White List is a matter of following these step-by-step instructions:

1. The administrator generates a cryptographic certificate (DeviceLock Certificate) using the Certificate Generation Tool (see [Generating DeviceLock Certificates](#)). A DeviceLock Certificate consists of two keys: private and public.

2. The administrator deploys the DeviceLock Certificate (the public key) to a user's computer. This enables the Temporary White List on the user's computer.
3. When a user needs to access some USB device, they run the [Temporary White List Authorization Tool](#) from the Windows Control Panel. Then, the user selects the particular device from a list and generates an alpha-numeric code (Device Code). The user provide that code to the DeviceLock Administrator (for example, over a phone or via an Internet chat session).
4. The administrator then runs the [DeviceLock Signing Tool](#), loads the respective DeviceLock Certificate (the private key), enters the Device Code, selects an appropriate temporary access period (5, 15, etc. minutes, until the device is unplugged or until the user is logged off), generates an Unlock Code, and relays that Unlock Code to the user.
5. Having received the Unlock Code, the user enters that Code into the [Temporary White List Authorization Tool](#). Access to the requested device is then granted for the specified period.

## Temporary White List Authorization Tool

To obtain temporary access to a device, the user should run the **DeviceLock** applet in Control Panel and select the **Temporary White List Authorization Tool** option.

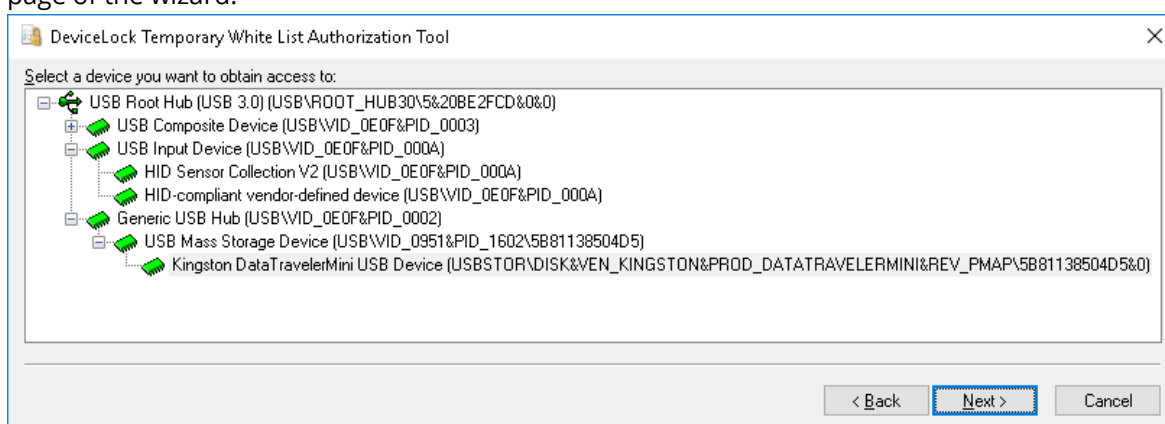


## Note

- To access the DeviceLock applet, the user has to switch Control Panel to the “Small icons” view mode.
- The caption of the applet window displays the DeviceLock version and build number.
- The DeviceLock applet may fail to start, returning the “Certificate is not installed” error. To resolve this issue, install the public key of the DeviceLock certificate on the client computer. For installation instructions, see [Installing/Removing DeviceLock Certificate](#).

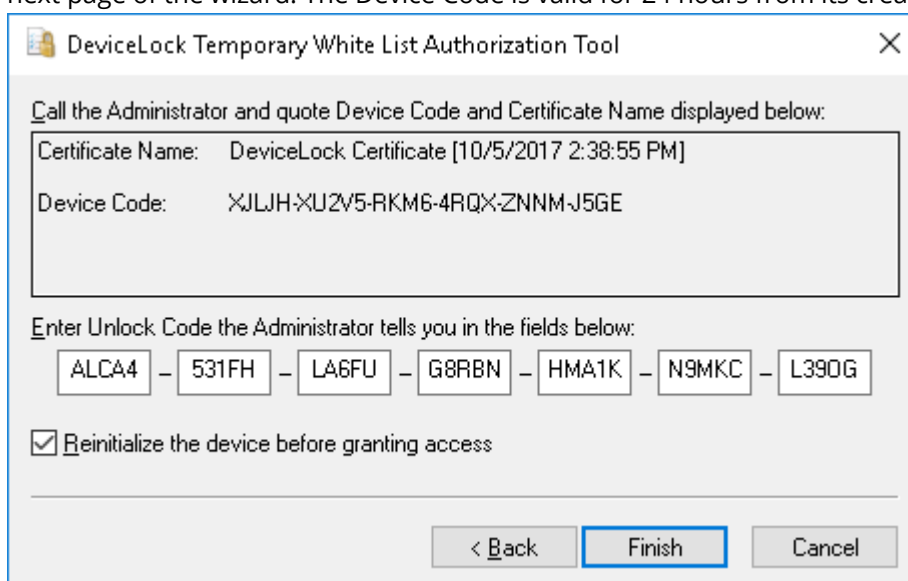
There are five simple steps for the user to request and obtain temporary access to a device:

1. Plug the needed device into the USB port.
2. Select the device from the list of all available USB devices and click **Next** to proceed to the next page of the wizard.



To assist in selecting the desired device, the wizard displays the device’s PID, VID and serial number (if any) in parentheses next to the name of the device.

3. Contact an Administrator and tell them the certificate name and the Device Code found on the next page of the wizard. The Device Code is valid for 24 hours from its creation.



4. Enter the Unlock Code received from the Administrator.

If access to the device requires it to reinitialize (replug), select the **Reinitialize the device before granting access** check box. Access to some USB devices (such as the mouse) cannot be provided without reinitializing, so it is recommended to select this check box for non-storage devices. It is also advisable to clear this check box for data storage devices (flash drives, optical drives, external hard drives, etc.).

---

**Important**

DeviceLock cannot reinitialize USB devices whose drivers do not provide for software replug of device. If there is no access to such a device, the user should remove the device from the USB port and then insert it back to restart the driver.

---

5. Click the **Finish** button.

If the user has entered a valid code, access to the device will be provided after a few seconds. The following message appears: "The device has been successfully unlocked for <time period>."

All successful attempts to add devices to a Temporary White List are logged, if the auditing of changes is enabled in [Service Options](#) (see the [Log Policy changes and Start/Stop events](#) parameter description).

# User Activity Monitor

## Introduction to User Activity Monitor

DeviceLock provides the ability to monitor end user actions by video recording the user's computer screen, as well as recording all keystrokes and information about the applications that were used on the computer during recording. With this kind of monitoring, DeviceLock helps expand the evidence base in the investigation of information security incidents, simplifies identifying suspicious user behavior, reveals misuse of access privileges or data protection policies, and therefore proactively mitigates possible risks of data leaks.

To implement user activity monitoring, the DeviceLock Service records the user's on-screen actions in a video format along with recording user keystrokes and saving other information such as active application name, active window title, and so on. The monitoring data can then be collected from user computers by the DeviceLock Enterprise Server where authorized persons can view and analyze those recordings of user activity.

The ability to store a recording of user actions gives DeviceLock a number of advantages when detecting data leak threats. The DeviceLock Service records exactly what the user sees on the computer screen regardless of applications and protocols used or level of privilege the user has. Keyboard input and other data recorded by DeviceLock Service along with video can be leveraged to track certain user actions.

The DeviceLock Service features various triggering criteria to start recording when certain events or conditions occur. Depending on the criteria selected in the policy, recording can start, for example, when a specific device is connected, a certain application is opened, or an unauthorized attempt is made to write a file or send a message. Triggering criteria enable the DeviceLock Service to perform selective recordings of potentially suspicious user actions. For a complete list of criteria, see [Setting up triggering criteria](#) later in this chapter.

DeviceLock Service initially stores user activity monitoring data on the local computer, allowing the administrator to explore local records of user actions in the DeviceLock Management Console connected to the DeviceLock Service. In this way, one can only view the records made by the DeviceLock Service on the local computer.

To enable a centralized viewing and analysis of the recordings made on different computers, it is necessary to transfer user activity monitoring data to DeviceLock Enterprise Server. The servers to collect and hold that data are specified by the respective DeviceLock Service setting. If necessary, the data from individual servers can be combined for viewing and analysis on a central collection server by using the log consolidation feature.

## Getting Started with User Activity Monitor

To leverage the user activity monitor, a DeviceLock administrator should first configure rules that cause the DeviceLock Service to start recording certain user activities. These rules are administered by using commands on the node **User Activity Monitor > Rules** in the DeviceLock Management

Console when connected to an endpoint's DeviceLock Service, or in the DeviceLock Service Settings Editor console or DeviceLock Group Policy Manager. The **Manage** command from the shortcut menu on that node opens a dialog box where rules are configured as follows:

1. Select users and/or groups to which the rule will apply. The recording of the activity of these users or groups begins when the trigger condition/s of this rule are met.
2. Add one or more triggering criteria to the rule. The triggering criteria added to the rule collectively determine the conditions under which the rule starts the recording of user activity.

For further details, see [Creating rules](#) later in this chapter.

The monitoring data captured by the DeviceLock Service is initially stored on the local computer, which allows the administrator to view local records of user actions in the DeviceLock Management Console connected to the endpoint's DeviceLock Service. This can be accomplished by using the **DeviceLock Service > User Activity Monitor > UAM Log Viewer** node.

---

### Important

DeviceLock Service might suspend monitoring of user activity due to insufficient disk space in the local data storage. For details, see [Local storage quota](#).

---

For a centralized viewing and analysis of the recordings made on different computers, it is necessary to transfer user activity monitoring data to the DeviceLock Enterprise Server. The servers to collect and hold that data must be specified by the [DeviceLock Enterprise Server\(s\)](#) option of the DeviceLock Service. In addition, the [Transfer shadow data to server](#) option must be set to **Enable**.

To view user activity monitoring records on the DeviceLock Enterprise Server, use the **DeviceLock Enterprise Server > UAM Log Viewer** node in the DeviceLock Management Console. The console displays a list of all user activity records available on the server, allowing authorized persons to view video recordings of computer screens along with records of keyboard input and other data related to user activity. For further details, see [Viewing User Activity](#) later in this chapter.

## Monitoring Settings

The DeviceLock Service settings relating to the user activity monitor are presented in the DeviceLock Management Console, in the DeviceLock Service Settings Editor console, and in the DeviceLock Group Policy Manager under the node **User Activity Monitor**:

- [Options](#) - Parameters common to all recording sessions. For example, determine whether to record color or only black and white video.
- [Rules](#) - Recording start/stop conditions and other parameters that may vary for different recording sessions. See also [Examples of user activity monitoring rules](#).

---

### Important

The User Activity Monitor feature requires the DeviceLock UAM volume license in addition to the DeviceLock Core license. For license installation instructions, see [Activating DeviceLock Licenses](#).

---

## Options

The user activity monitoring options are common parameters of user activity recording that are independent of start/stop conditions and other parameters being set by user activity monitoring rules. To view these specific user activity options in the details pane, select **DeviceLock Service > User Activity Monitor > Options** in the console tree of the DeviceLock Management Console or DeviceLock Service Settings Editor, or select **DeviceLock > User Activity Monitor > Options** if using the DeviceLock Group Policy Manager console.

The following options are available:

- **Grayscale** - Determines whether black & white or color recording will be performed.
- **Pause while inactive** - Determines whether to pause recording when the computer is not being used.
- **Video resolution** - Determines the resolution of the recorded video.
- **Multiple displays** - Determines how to perform screen recording on computers with multiple monitors.
- **Log passwords** - Determines whether to record user-entered passwords in clear text or replace them with asterisks.

## Grayscale

The **Grayscale** option determines the recording color mode. Enable the option to use black & white recording, which consumes less computer resources and makes a smaller volume of monitoring data. Disable this option if color recording is required.

## Pause while inactive

The **Pause while inactive** option gives the ability to suspend recording in the absence of user activity, which decreases the amount of monitoring data. When this option is enabled, recording is paused if the user does not press keys on the keyboard, does not move the mouse, nor clicks with it for some time. Recording resumes on any keystroke or mouse click/move. The value of this option specifies the maximum allowed inactivity time.

Double-click the option to view or change its value in the dialog box that appears:

- **Inactivity timeout** - The maximum period of time (number of seconds) that a user's session on a computer can be idle without user actions before the recording of this session is suspended. DeviceLock Service will automatically pause the recording of idle user sessions after the specified number of seconds.

To enable this option, set it to a non-zero value. The valid value is 3 or more seconds. To disable this option, set its value to 0. When this option is disabled, the DeviceLock Service continues recording even if there is no user activity.

---

## Note

This option has no effect on the rules that include the triggering criterion `Computer is idle for <number> seconds` (see [Setting up triggering criteria](#)). Such rules do not suspend recording after the inactivity time specified by this option expires.

---

## Video resolution

The **Video resolution** option allows the administrator to set the output resolution for the screen video recorded by the DeviceLock Service. This can be the resolution of the screen being recorded, or a different resolution selected from a list in the option setting.

Double-click this option to view or change its setting in the dialog box that appears:

- **Resolution** - Select the desired output resolution from the drop-down list for this setting.

For the output resolution to match the resolution of the screen being recorded, select **Native** from the **Resolution** list.

---

## Important

Recording maintains the aspect ratio of the screen being recorded, so the height or width of the resulting video may differ from that specified by the output resolution. Typically, the width matches the output resolution, and the height is calculated so as to preserve the original screen aspect ratio.

---

## Multiple displays

The **Multiple displays** option applies to computers with multiple displays, and it allows the administrator to specify whether to record the screen of a single monitor or the screens of all monitors. In the latter case, it is possible to combine all the monitors into one record or record each monitor separately.

Double-click this option to view or change the selection of its setting in the dialog box that appears:

- **Only the primary monitor** - Only the primary monitor screen is recorded.
- **All monitors as single file** - The screens of all monitors are recorded in a single record.
- **All monitors as separate files** - The screens of all monitors are recorded, with a separate recording made for each screen.

## Log passwords

The **Log passwords** option allows the administrator to secure user-entered passwords when recording keystrokes by replacing them with asterisks (\*).

Enable this option if it is acceptable to record passwords. As a result, passwords are recorded in plain text, which is then displayed and highlighted in red when [viewing the recording](#). Disable this option to avoid recording passwords. When this option is disabled, the keystroke recording viewer displays asterisks in place of passwords. The record in this case does not contain any password information, and one cannot view or recover passwords from such a record.



---

## Important

The **Log passwords** option has no effect when entering passwords in web forms. The passwords entered in web forms are recorded and displayed in clear text regardless of the option setting.



---

## Rules

User activity monitoring rules determine the conditions to start and stop recording the user activity. The recording of the activity of a given user begins when the conditions of the rule configured for that user are met, and stops when those conditions cease to be met. Different rules can be configured for different users or groups of users.





The users and groups for which monitoring rules are configured are listed in the console tree under **User Activity Monitor > Rules**. These users and groups are also listed in the details pane when the **Rules** node is selected in the console tree. To view which rules are configured for a specific user or group, select that user or group under the **Rules** node in the console tree. The list of the rules will appear in the details pane (see [Managing existing rules](#)).

The shortcut menu on the **Rules** node provides the following commands (next to the command name is the toolbar button corresponding to that command):

- **Manage**  - Opens a dialog box to set, view, or change the online mode rules (regular profile).
- **Manage Offline**  - Opens a dialog box to set, view, or change the offline mode rules (offline profile).

The dialog box for managing rules is similar for each of these two commands, but it manages different rule sets depending upon the command involved. For description of this dialog box, see [Dialog box for managing rules](#).

The offline mode rules take effect when the computer is not connected to the enterprise network; otherwise if offline mode is not configured or undefined, the online mode rules are applied in all cases. For details on how the DeviceLock Service determines whether the computer is connected to the enterprise network, see [Configuring Offline Mode Detection Settings](#).

- **Load**  - Imports rules from a file, and applies them for online mode. A dialog box opens to select the file to which the rules were saved.
- **Load Offline**  - Imports rules from a file, and applies them for offline mode. A dialog box opens to select the file to which the rules were saved.
- **Save**  - Exports the online mode rules to a file. A dialog box opens to specify the file to which the rules will be saved.
- **Save Offline**  - Exports the offline mode rules to a file. A dialog box opens to specify the file to which the rules will be saved.
- **Undefine Offline** - Deletes all offline mode rules, with the result that online mode rules will be applied both in online mode and offline mode.

These commands (with the exception of the **Undefine Offline** command) are also available in the shortcut menu on each user or group in the **Rules** node. In addition, the user/group menu includes the **Delete User** command intended to remove the selected user or group from the **Rules** node. For

the users and groups that have been removed from the **Rules** node, the effect of the rules is terminated.

In [DeviceLock Group Policy Manager](#) and [DeviceLock Service Settings Editor](#), the shortcut menu on the **Rules** node also includes the following commands:

- **Undefine** - Resets the online mode rules to the unconfigured state. Use this command to configure the DeviceLock Service settings so that the User Activity Monitor rules for regular profile are removed.
- **Remove Offline** - Blocks the inheritance of the offline rules and enforces the regular profile rules. Use this command to configure the DeviceLock Service settings so that the User Activity Monitor rules for regular profile are applied in both online mode and offline mode.

Management of monitoring rules involves the following activities:

- [Creating rules](#)
- [Managing existing rules](#)

## Creating rules

Creating a rule requires the following steps:

1. Execute the **Manage** or **Manage Offline** command from the shortcut menu on the node **User Activity Monitor > Rules**.  
This command opens a dialog box to add or remove users and groups as well as rules for their monitoring.
2. In the dialog box that appears, specify users or groups to which the rule is to apply, and then add and set up the rule. For details, see [Dialog box for managing rules](#).  
Adding a rule in the rules management dialog box opens a separate dialog box to set up the rule.
3. In the dialog box that appears, set up the recording's start condition and configure other rule settings. For further details, see [Dialog box for configuring a rule](#).

The **Manage** command is used for creating online mode rules. To create offline mode rules, use the **Manage Offline** command. The offline mode rules take effect when the computer is not connected to the enterprise network; otherwise, the online mode rules are applied. For details on how the DeviceLock Service determines whether the computer is connected to the enterprise network, see [Configuring Offline Mode Detection Settings](#).

## Dialog box for managing rules

The dialog box for managing rules appears when selecting the **Manage** or **Manage Offline** command on the shortcut menu of the node **User Activity Monitor > Rules** in the console. This dialog box provides for the following rule management tasks:

- View or change the list of the users and groups to which monitoring rules are applied.  
The list of the users and groups is shown on the left side of the dialog box. For each user or group from this list, one or more rules can be configured.  
Beneath the list are the management buttons:

- **Add** - Opens the standard dialog box provided by the operating system for selecting users and groups. The list adds users and groups selected in this dialog box.
- **Delete** - Removes the selected list item/s. For the users and groups that have been removed from the list, the effect of the rules is terminated.
- View, set, change, or remove rules for a particular user or group.  
Select a user or group in the list on the left side to view the rules for that user or group. The list of the rules appears on the right side of the dialog box. For each rule, the following information is listed:
  - **Name** - Indicates the name of the rule.
  - **Screen** - When this check box is selected, the rule causes the DeviceLock Service to perform video recording of the user's computer screen. Otherwise, video recording is not performed.
  - **Keylogger** - When this check box is selected, the rule causes the DeviceLock Service to record the sequence of keystrokes from the user's computer keyboard. Otherwise, the keystrokes are not recorded.

For each rule, one can select or clear check boxes directly in the list of rules.

Beneath the list of rules are the management buttons:

- **Add** - Opens a dialog box to configure the new rule.
- **Edit** - Opens a dialog box to view or change the rule selected in the list.  
The task of adding and editing rules is performed by using a dialog box described in the section [Dialog box for configuring a rule](#).
- **Delete** - Deletes the rule/s selected in the list. One can select multiple rules to delete at once.

---

#### Note

Deleting a rule normally does not interrupt the recording started by this rule and continuing at the time the rule was deleted. The rule's effect in this case ceases after the recording is completed. However, if the user is assigned only one rule, then deleting that rule interrupts the recording.

---

- Export or import rules from a file.  
The list of users and groups along with their rules can be exported to a text file. Click the **Save** button and then, in the dialog box that appears, specify the location and name of the file to hold the export data.  
The export file can be imported to a different computer, or it can be used as a backup copy of the rules. To import users, groups, and their rules from a file, click the **Load** button and open the file in the dialog box that appears.

### Dialog box for configuring a rule

The dialog box for configuring a rule appears when the **Add** or **Edit** button is clicked in the dialog box for managing rules, and provides the ability to set, view, or change the following rule settings:

- **Name** - Assigned when creating the rule, and it can be changed when editing the rule.
- **Description** - Any additional information about the rule (for instance, the intended purpose of the rule).
- **Capture** - DeviceLock Service records only the selected manifestations of the user activity:
  - **Screen** - When this check box is selected, the DeviceLock Service performs video recording of the user's computer screen.
  - **Keyboard Input** - When this check box is selected, the DeviceLock Service records the sequence of keystrokes from the user's computer keyboard.
- **Start capture when the following condition is true** - Recording of user activity starts depending upon the condition specified in the rule. The condition is a logical expression composed of one or more triggering criteria united by logical operators. Each of the criteria evaluates to either **true** or **false**. The condition value is calculated of the current values of its criteria, and the DeviceLock Service can start recording user activity only if this condition evaluates to **true**.

Some criteria from the recording start condition are also used to determine when to stop recording. For details, see [Ways to stop recording](#).

The dialog box provides a condition builder to add, change, or remove triggering criteria, to combine them by AND/OR, and to group by using brackets:

- Use the buttons above the criteria list to add or remove criteria and to change the order of criteria in the list:
  - **Add** - Adds new criteria to the end of the list. To add criteria, click this button or double-click a blank area in the list.
  - **Insert** - Adds new criteria before the one selected in the list.  
When adding criteria, first select its type, and then configure the criteria settings depending upon the selected type. For further details, see [Setting up triggering criteria](#).
  - **Edit** - Allows one to change the setting of the criteria selected in the list, or to replace the criteria with a different one. To start editing criteria, click this button or double-click criteria in the list.  
To edit criteria, a dialog box is used in which one can view/change the setting value of the selected criteria or choose another criteria to replace the criteria in the list. For further details, see [Setting up triggering criteria](#).
  - **Delete** - Removes the selected criteria from the list. This also removes the logical operators and brackets listed next to that criteria.
  - **^, v** (up and down arrows) - Move the selected criteria up and down in the list.  
Note that moving criteria up and down in the list may break the logical structure of the expression. Click the **Validate** button to check the syntax of the expression and display the resulting expression in the **Result** box.
- Select the check box in the **NOT** column to reverse the criteria value.
- Click in the column titled with a bracket ( **( or )** ) to add one or more brackets.  
Brackets are used to avoid ambiguity of expressions composed of multiple criteria. For example, the expression **A AND B OR C** could mean **(A AND B) OR C**, or it could mean **A AND (B OR C)**.

(B OR C). Use brackets to accurately determine the order and intention in which expressions are calculated.

---

**Note**

When moving an entry to the place of an adjacent one in the criteria list, the **NOT** check box setting moves together with the entry if the number of opening brackets is less than or equal to that of closing ones both in the moved entry and in the entry to which place it is moved. If at least one of them has more opening brackets than closing ones, the **NOT** check box setting does not move to the adjacent entry. Such a solution helps preserve the logical structure of the expression when the order of the list entries changes.

---

- Click in the **AND/OR** column to select the desired operator to combine the criteria into a logical expression. By default, AND is selected, so the recording starts when all the specified triggering criteria are met. Select OR if you want the recording to start when at least one of these criteria is met.
  - **Validate** - Checks the logical structure of the expression, removes unnecessary brackets if any, and displays the resulting expression in the **Result** box.
  - **Clear** - Removes all the triggering criteria from the condition, except the default one.
- 

**Note**

The recording start condition always contains the default criterion `User logged in`, which causes recording to start only if the user to whom the rule applies is logged on. This ensures that the actions of the logged-on user are recorded in accordance with the current rules for monitoring user activity.

---

- **Force stop capture in <number> seconds** - When this check box is selected, recording starts when the recording start condition is met, and then, after the specified number of seconds, it stops. If the recording start condition is still met, the recording starts again unless the following check box is selected:
  - **Do not run this rule again until its condition changes** - When this check box is selected, recording does not restart after being forced to stop by time even if the recording start condition is still met. In this case, recording restarts only after that condition will cease to be met and then occur to be met again. To clarify this behavior, let's suppose that recording starts when a certain process gets running in the operating system, and then, after some time, recording is forcibly stopped. To restart recording in this case, one would need to stop that process and then start it again.

More on these two settings see in [Ways to stop recording](#).

- **Timeout between screenshots: <number> seconds** - Determines the frequency of screen shots in the video. Having taken a screen shot, the DeviceLock Service waits the specified number of seconds before taking the next shot to decrease the odds of video frames with exactly the same contents.

The last specified value of this setting is used as the convenient default value when creating new rules. Suppose, for example, a value of 3 had been set for a certain rule. After that, the value of 3 will be used by default in all newly created rules until another value is set in some rule.

---

**Note**

This setting requires the **Capture > Screen** check box to be selected. Otherwise, this setting is unavailable (grayed out), and has no effect on recording.

---

## Setting up triggering criteria

When configuring a rule, the administrator specifies a recording start condition that is composed of triggering criteria united by logical operators. Each of these criteria corresponds to a certain system state or event in which it is met and therefore evaluates to `true` (for details, see [System state criteria vs. event criteria](#)). The condition value is calculated of the current values of its criteria, and recording can start only if the condition evaluates to `true`.

The system state criteria from the recording start condition are also used to determine when to stop recording. For details, see [Ways to stop recording](#).

A rule can specify one or more triggering criteria that enable recording to be started in different situations, such as when connecting devices, starting applications, or triggering DeviceLock policies. The rule's criteria are listed in the dialog box where the administrator can add, edit, or remove triggering criteria from a rule (see [Dialog box for configuring a rule](#)).

The dialog box for setting up triggering criteria is used in the following cases:

- When adding criteria to the rule, the desired criterion can be selected from a drop-down list. Then, depending upon which criterion is selected, the dialog box provides a field to set a configurable value for the selected criterion.
- When editing criteria specified in the rule, the dialog box displays the selected criterion and its current setting value, if any. One can view/change the setting value, or choose a different criterion to replace the current one.

The following list briefly describes the triggering criteria and their settings.

- **User logged in** - The monitored user logged on to the computer or logged on remotely using Terminal Services or Remote Desktop, and was successfully authenticated.

---

**Note**

This criterion is included in each condition by default and cannot be removed, therefore it is not in the list for selecting criteria.

---

- **Ethernet connection exists** - Network cable is plugged in to the computer.
- **VPN connection exists** - The computer is connected to a virtual private network (VPN).
- **Wireless connection exists** - The computer is connected to a wireless network via Wi-Fi.
- **IP address is assigned** - A network interface on the computer has received an IP address.
- **IP address is released** - A network interface on the computer has released its IP address.

- **Process "<name>" exists** - The computer is executing the specified process started by the monitored user.  
Setting to configure: The path and name of the process executable file (for example, c:\mypath\process.exe). The setting allows the use of wildcards: an asterisk (\*) for an arbitrary series of characters, a question mark (?) for any single character.

---

**Note**

If it is necessary for this criterion to work regardless of the path to the process executable, specify the file name as follows: \*\<file name>. Example: \*\excel.exe

---

- **Window "<title>" exists** - The system has a window with the specified title, opened by the monitored user.  
Setting to configure: Window title. The setting allows the use of wildcards: an asterisk (\*) for an arbitrary series of characters, a question mark (?) for any single character.
- **Window "<title>" is focused** - A window with the specified title, which was opened by the monitored user, is active and can receive keyboard and mouse input.  
Setting to configure: Window title. The setting allows the use of wildcards: an asterisk (\*) for an arbitrary series of characters, a question mark (?) for any single character.
- **Content-Aware rule "<name>" is triggered** - The monitored user tried to send or receive data that matches the Content-Aware rule with the specified name.  
Setting to configure: Rule name. The setting allows the use of wildcards: an asterisk (\*) for an arbitrary series of characters, a question mark (?) for any single character.

---

**Note**

This criterion applies only to content-aware rules for access control or detection. It disregards the rules for content-aware shadowing.

---

- **Protocol White List rule "<name>" is triggered** - The monitored user tried to use a white-listed protocol that matches the white list rule with the specified name.  
Setting to configure: Rule name. The setting allows the use of wildcards: an asterisk (\*) for an arbitrary series of characters, a question mark (?) for any single character.
- **Media White List rule "<description>" is triggered** - The monitored user tried to access white-listed media with the specified description.  
Setting to configure: Media description. The setting allows the use of wildcards: an asterisk (\*) for an arbitrary series of characters, a question mark (?) for any single character.
- **USB White List rule "<description>" is triggered** - The monitored user tried to access a white-listed USB device with the specified description.  
Setting to configure: Device description. The setting allows the use of wildcards: an asterisk (\*) for an arbitrary series of characters, a question mark (?) for any single character.
- **Storage device is attached** - The monitored user attached any of these device types to the computer: Removable, MTP, iPhone, Floppy, Optical Drive, TS Devices (mapped drive).
- **Non-storage device is attached** - The monitored user attached any device type to the computer, except Removable, MTP, iPhone, Floppy, Optical Drive, TS Devices (mapped drive).

---

### Important

This criterion does not trigger the recording of user activity upon attaching USB HID devices (keyboard, mouse, etc.).

---

- **Computer is idle for <number> seconds** - The computer is not screen-locked, and there is no activity of the monitored user on this computer for the specified time.  
Setting to configure: The time period of user inactivity (number of seconds) after which this criterion deems to be met. The setting value must be 3 or more seconds.

---

### Note

The option [Pause while inactive](#) has no effect on the rules with this criterion in the recording start condition. Rules with such a condition do not suspend recording after the time specified by that option expires.

---

- **Read access to "<name/s>" is denied** - DeviceLock has blocked an attempt of the monitored user to receive data due to a deny on access to one of the specified devices / protocols, or according to one of the specified security settings.  
Setting to configure: List of device, protocol and/or security setting names. The desired names can be selected from a drop-down list.
- **Write access to "<name/s>" is denied** - DeviceLock has blocked an attempt of the monitored user to send data due to a deny on access to one of the specified devices / protocols.  
Setting to configure: List of device and/or protocol names. The desired names can be selected from a drop-down list.

### ***More on some triggering criteria***

The value of the `Storage device is attached` criterion is true as long as one or more devices of any of the following types is attached to the computer:

- Removable - For example, a USB stick is connected.
- MTP - For example, a USB media player is connected.
- iPhone - An iPhone or iPad is connected.
- Optical Drive - An optical disc is inserted into the disc drive.
- Floppy - A floppy disk is inserted into the disk drive.
- TS Devices (mapped drive) - A hard/removable/optical disk is connected in the remote desktop/application session on a virtualization server (Remote Desktop Server, Citrix XenDesktop/XenApp, etc.).

The `Storage device is attached` criterion evaluates to false if none of the above device types is attached to the computer.

In the case of access to devices, `Read access to "<name/s>" is denied` criteria evaluate to true when attempting any of the following:

- Actions denied by "generic" access rights such as Read, Mapped Drives Read, Serial Port Access, USB Devices Access, Clipboard Incoming Text / Image / Audio / File / Unidentified Content (see



[“Generic” Rights Category](#)).

- Actions denied by the “encrypted” access right Read (see [“Encrypted” Rights Category](#)).
- Actions denied by “special permissions” such as Read Calendar / Contact / E-mail / Attachment / Favorite / File / Media / Backup / Note / Pocket Access / Task / Expense / Document / Unidentified Content (see [“Special Permissions” Rights Category](#)).

In the case of access to protocols, Read access to “<name/s>” is denied criteria evaluate to true when attempting any of the following:

- Actions denied by protocol access rights such as Send/Receive Data, Web Send/Receive Data, Search, Incoming Files, Incoming Calls (see [Access Rights](#) for protocols).
- Actions denied by protocol security settings, provided that appropriate item/s are selected in the criteria setting:
  - Block unrecognized outgoing SSL traffic - Select SSL in the criteria setting.
  - Block IP addresses in URL - Select IP (TCP) and/or IP (UDP) in the criteria setting, depending upon which transport protocol/s (TCP / UDP) this criterion should respond to.
  - Block proxy traffic - Select Proxy (HTTP), Proxy (SOCKS4), and/or Proxy (SOCKS5) in the criteria setting, depending upon which proxy server type/s (HTTP / SOCKS4 / SOCKS5) this criterion should respond to.
  - Block Tor Browser traffic - Select Tor Browser in the criteria setting.

For details on security settings for protocols, see [Security Settings Description](#).

In the case of access to devices, Write access to “<name/s>” is denied criteria evaluate to true when attempting any of the following:

- Actions denied by “generic” access rights such as Write, Format, Print, Copy to clipboard, Mapped Drives Write, Clipboard Outgoing Text / Image / Audio / File / Unidentified Content (see [“Generic” Rights Category](#)).
- Actions denied by “encrypted” access rights such as Write, Format (see [“Encrypted” Rights Category](#)).
- Actions denied by “special permissions” such as Write Calendar / Contact / E-mail / Attachment / Favorite / File / Media / Backup / Note / Pocket Access / Task / Expense / Document / Unidentified Content, Copy Text / Image / Audio / File / Unidentified Content, Screenshot (see [“Special Permissions” Rights Category](#)).

The Write access to “<name/s>” is denied criteria have no effect when denying access to the following device types: Blackberry, Bluetooth, Infrared port, Serial port, Parallel port, TS Devices in case of denying Serial Port Access or USB Devices Access, and WiFi. You can use the Read access to “<name/s>” is denied criteria to start recording upon denying access to these devices.

In the case of access to protocols, the Write access to “<name/s>” is denied criteria evaluate to true when attempting any of the actions denied by protocol access rights such as Outgoing Messages, Outgoing Files, POST Requests, Outgoing Calls (see [Access Rights](#) for protocols).

## System state criteria vs. event criteria

There are two types of triggering criteria: system state criteria are driven by the current state of the system whereas event criteria are driven by certain events occurring in the system.

System state criteria retain the value `true` as long as some objects exist in the system, and switch to `false` only when the object disappears. For example, the criterion `Process "<name>" exists` retains the value `true` throughout the running of the specified process. The value of this criterion changes to `false` upon the end of the process and remains so until the process is started again. So behave all triggering criteria that are driven by the existence of certain system objects (in this example, processes running in the system).

Event criteria evaluate to `true` when certain events occur in the system, and switch to `false` shortly after the event has occurred. For example, the criterion `Write access to "<name/s>" is denied` evaluates to `true` when DeviceLock Service blocks an attempt to transfer data using the specified devices / protocols. Then, after some time, the criterion value changes back to `false`, and remains so until a new attempt to transfer data is blocked. So behave all triggering criteria that are driven by certain events in the system.

---

### Note

Since event criteria take the value of `true` for very short time, their combination by AND logic would always have the value of `false`. Therefore, it makes no sense to combine event criteria by AND logic.

---

The following are system state criteria:

- User logged in - `true` all the time until the user logs out.
- Ethernet connection exists - `true` all the time while the connection exists.
- VPN connection exists - `true` all the time while the connection exists.
- Wireless connection exists - `true` all the time while the connection exists.
- Window "`<title>`" exists - `true` all the time while this window exists.
- Window "`<title>`" is focused - `true` all the time until the input focus moves away from this window.
- Process "`<name>`" exists - `true` all the time while this process exists.
- Storage device is attached - `true` all the time while the device is attached.
- Non-storage device is attached - `true` all the time while the device is attached.
- Computer is idle for `<number>` seconds - `true` all the time after triggering while the user does not press keys on the keyboard and does not move/click the mouse.

The following are event criteria:

- IP address is assigned - `true` for a short time after the address is assigned.
- IP address is released - `true` for a short time after the address is released.
- Content-Aware rule "`<name>`" is triggered - `true` for a short time after this rule is triggered.
- Protocol White List rule "`<name>`" is triggered - `true` for a short time after this rule is triggered.
- Media White List rule "`<description>`" is triggered - `true` for a short time after this rule is triggered.

- USB White List rule “<description>” is triggered - true for a short time after this rule is triggered.
- Read access to “<name/s>” is denied - true for a short time after read access is denied.
- Write access to “<name/s>” is denied - true for a short time after write access is denied.

## Ways to stop recording

User activity monitoring rules provide the following ways to control the start and stop of recording:

- The recording start condition, according to which the DeviceLock Service can start recording only if this condition evaluates to true.

The part of the recording start condition that includes only the system state criteria, referred to as the *recording run condition*, is also used to control when to stop recording. If the recording run condition evaluates to false, the recording stops.

Consider, for example, the following recording start condition:

Window “<title>” exists AND Content-Aware rule “<name>” is triggered

The recording run condition in this case is Window “<title>” exists. It does not include Content-Aware rule “<name>” is triggered as this is an event criterion rather than a system state one. For details on the two types of triggering criteria, see [System state criteria vs. event criteria](#).

For more information, see [How the recording run condition is calculated](#).

- The **Force stop capture** setting causes the DeviceLock Service to stop recording once the specified time has expired, regardless of the recording run condition.
- The **Do not run this rule again until its condition changes** setting, according to which the DeviceLock Service does not restart recording, stopped after a specified time, until the value of the recording start condition changes to false and then back to true.

DeviceLock Service stops the recording of the user’s activity if:

- The recording run condition value has changed to false.  
- OR -
- The time specified by the **Force stop capture** setting has expired.

This results in the following user activity monitoring rule features described:

- If the **Force stop capture** check box is not selected, the recording will continue as long as the recording run condition value is true. Suppose, for example, the recording start condition contains only the default criterion - User logged in, and the **Force stop capture** check box is not selected. In this case, the recording will continue until the user logs off.
- If the recording start condition contains only event criteria in addition to the default one, and the **Force stop capture** check box is not selected, then recording will start upon occurrence of the specified events and continue until the user logs off. In this case, for the recording to stop after a certain time, one should select the **Force stop capture** check box.
- If the **Force stop capture** check box is selected, the recording will stop when the time specified by this setting expires, even if the recording run condition value is true. In this case, the rule with the default recording start condition will stop the recording after the specified time, and then start the recording again as long as the user remains logged on. For the recording not to restart, one should select the **Do not run this rule again until its condition changes** check box. With

this check box selected, the recording will not restart until the user logs off and then logs on again.

### ***How the recording run condition is calculated***

The recording run condition governs the end of the recording session. The recording stops when the value of this condition changes to `false`. At the beginning of the session, this value equals to the value of the recording start condition. During the session, this is the value of the logical expression representing the recording start condition in which the values of the event criteria are frozen as of the time that the recording started. The recording run condition is calculated by passing into that expression the current values of the system state criteria held in the recording start condition.

Formally, the value of the recording run condition is calculated as follows. Let's denote the logical expression of the recording start condition by  $F(e, s)$  where  $e$  and  $s$  represent the current values of the event criteria and system state criteria, respectively. The recording run condition current value is the value of the logical expression  $F(e0, s)$  where  $e0$  represents the values of the event criteria as of the time of the recording session start.

## **Examples of user activity monitoring rules**

The following examples show how user activity monitor works in some typical usage scenarios. They help to better understand the behavior of some triggering criteria, their role in the recording start conditions and interrelation with other monitoring settings, and the conditions that cause recording to stop.

### ***Example 1: Recording starts immediately after the user logs in***

To record user activity, it is required that the user be logged in and authenticated. Therefore, each user activity monitoring rule always contains a condition to start recording upon user login. Thus, if a rule is specified without any additional triggering criteria, the DeviceLock Service will start recording immediately after the user successfully logs on and authenticates to the domain or to the local PC.

To record user activity for a specific time after the user logs in, configure a rule with the following settings:

- User logged in - Recording start condition, specified by default.
- Force stop capture in <number> seconds - Check box selected.
- Do not run this rule again until its condition changes - Check box selected.

Thus, to record for at most an hour, a value of 3600 seconds must be specified:

Force stop capture in 3600 seconds

With this rule, recording starts as soon as the user logs in, and stops either after an hour or earlier in case of user logout in less than an hour. The next time recording starts after the user logs out and then logs back in.

### ***Example 2: Application usage recording starts upon VPN connection***

The DeviceLock Service can be configured to record the user's activity in a situation where a certain application is running and a virtual private network (VPN) connection is established. The respective recording start condition looks as follows:

Process "<name>" exists AND VPN connection exists

Thus, to record when using Excel, the executable file's name excel.exe must be specified:

Process "\*\excel.exe" exists AND VPN connection exists

Because of AND logic, recording does not start when using Excel without VPN. However, once VPN is connected, DeviceLock will be recording the user activity as long as Excel is running. Recording will stop upon closing Excel or disconnecting VPN.

### ***Example 3: Time-limited recording starts upon Wi-Fi connection***

Another example is to configure the DeviceLock Service to record the user's activity for a certain time period after establishing a wireless network connection. The rule settings in this case are as follows:

- Wireless connection exists - Recording start condition.
- Force stop capture in <number> seconds - Check box selected.
- Do not run this rule again until its condition changes - Check box selected.

Thus, to record for at most 30 minutes after establishing a wireless network connection, a value of 1800 seconds must be specified:

Force stop capture in 1800 seconds

Such a rule starts recording once a wireless network has connected. In this example, recording lasts no more than 30 minutes and stops either after 30 minutes or earlier, in case of a disconnection from the wireless network in less than 30 minutes. Recording will start again only after disconnecting from and then re-connecting to a wireless network.

### ***Example 4: Recording starts upon running a particular application***

Let us consider a rule that would start recording, depending on whether a particular application is running, that is, recording starts if the respective process name or window caption is present in the system. Here is the recording start condition for such a rule:

- Process "<name>" exists - Application identified by process name.
- Window "<title>" exists - Application identified by window title.

If the DeviceLock Service is already running when the application is started, it will notice that the specified process or window has appeared on the system, and will start recording. However, certain processes may be up and running before the start of the DeviceLock Service, for instance, when the DeviceLock Service starts on a system that has already been running for some time. In this case, the DeviceLock Service searches the system for the processes and windows referenced in its user activity monitor rules, and starts recording as those rules require. Hence, the rules respond to the presence of a process or window in the system rather than to the fact of its appearance.

### ***Example 5: Recording starts on user inactivity***

This example covers a rule that causes DeviceLock to start recording if the computer is not screen-locked and it is not being used for a certain time period. The rule triggers when the user does not press keys on the keyboard, does not move the mouse, nor clicks with it for some time. In contrast to the option [Pause while inactive](#), this rule starts rather than suspends recording in the absence of user activity. The recording start condition looks as follows:

Computer is idle for <number> seconds

Thus, for recording to start after 5 minutes of user inactivity, a value of 300 seconds must be specified:

Computer is idle for 300 seconds

If such a rule is in effect, recording starts when, for the specified time on the computer, there are no keystrokes or mouse clicks/moves, while the computer is not screen-locked. Recording stops once any activity using the keyboard or mouse has occurred on that computer.

### What if a rule triggers when recording is in progress?

Suppose rule A starts a recording of the actions of a certain user, and during that recording rule B triggers to record the actions of the same user. In such a situation, rule B does not start a new recording if both rules are configured to record video. This situation is considered in more detail in the following table.

Rule A settings	Rule B settings	Outcome of rule B triggering
Record video only	Record video only	New recording does not start. Recording started by rule A is continued so long as it should according to rule A and rule B, and it ends only after both rules stop recording.
Record both video and keystrokes	Record both video and keystrokes	
Record video only	Record both video and keystrokes	Previously started recording continues. Information about keystrokes is added to it according to rule B.
Record both video and keystrokes	Record video only	Previously started recording continues. Information about keystrokes is added to it according to rule A.
Record keystrokes only	Record video and/or keystrokes	Rule B starts a new recording. Rule A continues the recording it started.
Record video and/or keystrokes	Record keystrokes only	

If several other rules (B, C, . . . ) triggered during recording started by some rule A, then a new recording does not start only if each rule A, B, C, ... records video and, possibly, keystrokes. Otherwise, a new recording of video and/or keystrokes may start. The rules that triggered during video recording without starting a new recording are listed on the watermark of the video, as well as in the **Rule** field of the UAM Log Viewer (see [List of Monitoring Sessions](#)). Video recording continues according to the rules that triggered, and it ends only after all those rules stop recording. Keystrokes are recorded as needed in accordance with the settings of those rules.

Suppose a certain rule starts a recording of user actions, and during that recording the same rule triggers again for the same user. In this case, a new recording does not start even if the rule in question is configured to record keystrokes only. Recording will continue in accordance with the new triggering of the rule. The rule triggering time offset shows up in square brackets in the **Rule** field of the UAM Log Viewer (see [List of Monitoring Sessions](#)).

### What if there is nothing to record?

The triggering of the rule does not lead to the creation of a record in the UAM Log if the DeviceLock Service has not managed to register any user actions for the entire duration of the recording. This situation is considered in more detail in the following table.

Rule is configured to capture	What happened during recording
Screen only	DeviceLock Service did not take any screenshots.
Keyboard Input only	DeviceLock Service did not register a single keystroke.
Screen and Keyboard Input	DeviceLock Service did not take any screenshots and did not register a single keystroke.

In all cases listed in the table, a record is not created in the UAM Log.

### Managing existing rules

The users and groups with the configured user activity monitoring rules are listed in the console tree under **User Activity Monitor > Rules**, and also in the details pane when the **Rules** node is selected in the console tree. To view the rules for a user or group, select that user or group in the console tree, or double-click the user or group in the details pane. As a result, the details pane lists the rules for the given user or group, with the following information on each rule:

- **Name** - Displays the name of the rule. The name is assigned when creating the rule, and it can be changed when editing the rule.
- **Description** - Displays the description of the rule. Description may provide any additional information about the rule (for example, the purpose of the rule). A description can be set or changed when creating or editing the rule.
- **Screen Capture** - Indicates whether the rule causes the DeviceLock Service to perform video recording of the user's computer screen. This option can be set or changed when creating or editing the rule.

- **Keylogger** - Indicates whether the rule causes the DeviceLock Service to record the sequence of keystrokes from the user's computer keyboard. This option can be set or changed when creating or editing the rule.
- **Condition** - Indicates the recording start condition specified in the rule. The condition is a logical expression composed of one or more triggering criteria united by logical operators. Recording starts when this expression evaluates to true. The condition can be set or changed when creating or editing the rule.

---

#### Note

As the condition always contains the criterion `User logged in`, the **Condition** field normally does not display this well-known criterion. It is displayed only if the condition does not contain other triggering criteria.

---

- **Profile** - Possible values:
  - **Regular** - The rule is applied when the computer is connected to the enterprise network (online mode rule). This profile is assigned to the rules created by using the **Manage** command.
  - **Offline** - The rule is applied when the computer is disconnected from the enterprise network (offline mode rule). This profile is assigned to the rules created by using the **Manage Offline** command.

The profile is assigned when creating the rule, and it cannot be changed once the rule has been created.

For details on how the DeviceLock Service determines whether the computer is connected to the enterprise network, see [Configuring Offline Mode Detection Settings](#).

The shortcut menu on a user or group provides all the commands from the shortcut menu of the [Rules](#) node, with the exception of the **Undefine Offline** command. In addition, it includes the **Delete User** command intended to remove the user or group from the **Rules** node. For the users and groups that have been removed from the **Rules** node, the effect of the rules is terminated.

The shortcut menu on a rule in the details pane provides the following commands:

- **Manage** - Opens a dialog box to set, view, or change user activity monitoring rules. In the case of selecting this command on a regular-profile rule, a dialog box opens for managing the online mode rules. In the case of selecting this command on an offline-profile rule, a dialog box opens for managing the offline mode rules. The dialog box looks similar in each of these two cases, but it serves to manage different rule sets depending upon the profile of the rule on which the **Manage** command is selected. For description of this dialog box, see [Dialog box for managing rules](#).
- **Edit** - Opens a dialog box to view or change the rule selected in the list. For description of this dialog box, see [Dialog box for configuring a rule](#).
- **Screen Capture** - Toggles the rule's setting that controls the video recording of the user's computer screen. Click this command to turn the video recording on or off. If multiple rules are



selected, the **Enable Screen Capture / Disable Screen Capture** commands are displayed instead of this command.

- **Keylogger** - Toggles the rule's setting that controls the recording of keystrokes on the user's computer keyboard. Click this command to turn the keystrokes recording on or off. If multiple rules are selected, the **Enable Keylogger / Disable Keylogger** commands are displayed instead of this command.
- **Delete** - Deletes the rule/s selected in the list. One can select multiple rules to delete at once.

---

#### Note

Deleting a rule normally does not interrupt the recording started by this rule and continuing at the time the rule was deleted. The rule's effect in this case ceases after the recording is completed. However, if the user is assigned only one rule, then deleting that rule interrupts the recording.

---

## Viewing User Activity

The DeviceLock Service initially stores user activity monitoring data on the local computer, allowing the administrator to explore local records of user actions by using the UAM Log Viewer in the DeviceLock Management Console connected to the DeviceLock Service. In this way, one can only access the records made by the DeviceLock Service on the local computer.

To enable a centralized viewing and analysis of the recordings made on different computers, it is necessary to transfer user activity monitoring data to DeviceLock Enterprise Server by enabling the [Transfer shadow data to server](#) option of the DeviceLock Service. The servers to collect and hold that data are specified by the [DeviceLock Enterprise Server\(s\)](#) option. Each server collects the data relating to only the users and groups assigned to that server. If necessary, user activity records can be combined for viewing and analysis on a central collection server (see [Consolidating Logs](#)).

User activity monitoring data is stored in the same place as shadow files. The DeviceLock Service stores them in the folder specified by the [Local storage directory](#) option. As for the DeviceLock Enterprise Server, the data storage is determined by the **Store path** option (see [Server Options](#)). For more information about server data storage options, see the [Store shadow files in the database](#) option description.

The administrator can view user activity monitoring records in the DeviceLock Management Console details pane, having selected **UAM Log Viewer** in the console tree. To view local records, select **DeviceLock Service > User Activity Monitor > UAM Log Viewer** in the console connected to the DeviceLock Service. To view records on the server, select **DeviceLock Enterprise Server > UAM Log Viewer** in the console connected to the DeviceLock Enterprise Server. The log can be administered by using shortcut menu commands on the **UAM Log Viewer** node (see [Managing the UAM Log](#)).

The viewer details pane is divided into upper and lower areas. The upper area displays a [list of monitoring sessions](#) - a listing of all user activity records held in the log. The lower area is a [session](#)

[viewer](#) intended to view the video recording of the user computer screen along with the recording of user keystrokes and other data.

---

### Important

- To collect UAM data, the DeviceLock Enterprise Server must have the Core license installed. The number of computers from which the server collects UAM data cannot be more than the Core license specifies.
- To apply server policies and computer monitoring tasks that include UAM options and rules, the DeviceLock Enterprise Server must have the UAM license installed. The number of computers to which such policies and tasks are applied cannot be more than the UAM license specifies.

For license installation instructions, refer to [Activating Server Licenses](#).

---

## List of Monitoring Sessions

To view user activity, select **UAM Log Viewer** in the console tree. The upper part of the details pane contains a list of user activity records - monitoring sessions stored in the log. For each record, the list provides the following information:

- **Computer** - The name of the computer on which this monitoring session was recorded. The computer name is displayed only in the log on the DeviceLock Enterprise Server. It is not displayed in the log on the DeviceLock Service.
- **Date/Time** - The date and time that the recording of this session started.
- **Type** - The types of recording available in this session. Possible values:
  - **Video** - The computer screen video recording only.
  - **Keylogger** - The computer keystrokes recording only.
  - **Video, Keylogger** - The computer screen recording and keystrokes recording.

---

### Note

If the session contains only screen recording or only keystroke recording, the session type is **Video** or **Keylogger**, respectively, even if the monitoring rule is configured to capture both the computer screen and keystrokes. This happens, for example, when the DeviceLock Service fails to take screenshots or capture keystrokes during recording.

---

- **Rule** - The name of the rule that caused the recording. Multiple rules could be listed here if more than one rule triggered during this recording.
  - **Reason** - The triggering criteria of the rule that caused the recording. In case of multiple rules, a separate list of triggering criteria is specified for each rule.
- 

### Note



As the rule always has the triggering criterion `User logged in`, the **Reason** field normally does not display this well-known criterion. It is displayed only if the rule does not have other triggering criteria.

---

- **Duration** - The time span (hours, minutes and seconds) that recording lasted.

- **User** - The name of the user whose activity is recorded in this session.
- **Received Date/Time** - The date and time that the DeviceLock Enterprise Server received this record from the DeviceLock Service.  
The received date and time is displayed only in the log on the DeviceLock Enterprise Server. It is not displayed in the log on the DeviceLock Service.
- **Server** - The name of the DeviceLock Enterprise Server computer that received this record from the DeviceLock Service.  
The server name is displayed only in the log on the DeviceLock Enterprise Server. It is not displayed in the log on the DeviceLock Service.
- **Consolidation Server** - The name of the remote server from which this record was last received during log consolidation (see [Consolidating Logs](#)).
- **Consolidated Date/Time** - The date and time that this record was last received from the remote server during log consolidation (see [Consolidating Logs](#)).  
The consolidation-related information is displayed only in the log on the DeviceLock Enterprise Server. It is not displayed in the log on the DeviceLock Service.

On each record, the shortcut menu provides the following record management commands (next to the command name is the toolbar button corresponding to that command):

- **Open** - Opens the recorded file in the application that is registered for the given file type in the operating system. If the session contains screen recording, this command opens the recorded video file. If the session contains only keystroke recording, this command opens the file where keystrokes are recorded.
- **Save**  - Saves the recorded video and/or keyboard input (keylog) to the file/s you specify. The keylog (if exists) is saved as an HTML file.
- **Delete**  - Deletes the selected record/s. Use the Ctrl and Shift keys to select and delete multiple records at a time.

The shortcut menu on each record also includes the log management commands listed in [Managing the UAM Log](#).

Use filtering to look for sessions of interest (see [Filtering the list of sessions](#)). Select a session in the list to view its recording (see [Session Viewer](#)).

## Filtering the list of sessions

When the **UAM Log Viewer** node is selected in the console tree, the details pane lists all available monitoring sessions. The following tools can be used to look for specific sessions in this list:

- The **Quick filters** command leaves only sessions for a certain period (day, week, month, year) in the list. For more on this command, see [Managing the UAM Log](#).
- The **Filter** command narrows the list in accordance with the specified conditions (recording date, user name, recorded data, etc.). For further details, see [UAM log filter](#).

## Session Viewer

Select the **DeviceLock Enterprise Server > UAM Log Viewer** node in the console tree, and then select a monitoring session from the list in the details pane to view the following in the lower part of the details pane:

- **Screen recording** - A video player shows the recording of the user's computer screen, if the session rule was set to capture screen.
- **Keystroke recording** - A table shows the records of the user's keystrokes, if the session rule was set to capture keystrokes.
- **Process list** - A separate table lists all processes run by the monitored user during this session.

To start viewing a monitoring session, double-click that session in the list. To administer sessions, use the commands from the session shortcut menu (see [List of Monitoring Sessions](#)).

### Screen recording viewer

To play back the recording of the computer screen, use the video player in the lower area of the details pane. To start playback, select the desired monitoring session in the list on the details pane and click inside the video player, or double-click the monitoring session in the list.

The following video viewing controls are located at the bottom of the player:

- Playback control button - Located in the lower left corner. Click this button to start / pause / resume playback.
- Playback progress / seek bar - Use the bar above the control button to:
  - View the playback progress. A moving knob in the bar indicates the current position of progress through the recording's playback time.
  - View the playback time line. Hover over the knob / bar to display the time in minutes and seconds from the beginning of the recording to the respective position on the bar.
  - Start playback from a specific point in the recording. Drag the knob or click in the bar to move to the desired position in the recording's playback time.
- Current playing time / total video duration - Displayed next to the control button in the format min:sec / min:sec.
- Full screen button - Located in the lower right corner. Click this button to expand the video to full screen. To exit full-screen mode, press the Esc key.

The arrow keys can be used to scroll through the video during playback. Press the left arrow key to rewind 10 seconds; press the right arrow key to fast forward 10 seconds. To rewind or fast forward continuously, hold down the left arrow or right arrow key, respectively.

The player may include multiple tabs in case of multiple displays on the user's computer. Each tab plays the screen recording of a particular display if there is a separate recording for each display according to the [Multiple displays](#) option.

## Keystroke recording viewer

A table in the lower part of the details pane displays records of the user's keystrokes, with the following information on each record:

- **Date/Time** - The date and time the user started typing.
- **Window Title** - The title of the application window into which the user typed.
- **Keyboard Input** - The characters the user typed and, optionally, the names of the pressed non-character keys.
- **Process Name** - The name and path of the executable file of the application into which the user typed. The process identifier (PID) is displayed in parentheses after the file name.

By default, **Keyboard Input** displays only the characters the user typed. Non-character keys the user pressed (such as Shift, Alt, Enter, Right, Left, etc.) are skipped. To view all recorded keystrokes, select the **Show specials** check box. With this check box selected, the viewer displays both the typed characters and the names of non-character keys the user pressed, with the names of non-character keys enclosed in square brackets (for example, [Shift]serial number).

If the recording was performed with [Log passwords](#) enabled, **Keyboard Input** also displays in red the passwords the user entered; otherwise, it displays asterisks in place of passwords.

---

### Note

When entered in the **Windows Security** dialog box, the user name and password are logged together. Therefore, in this case, the user name is also highlighted in red or replaced with asterisks in **Keyboard Input**, depending upon whether [Log passwords](#) was enabled during recording.

---

The viewer provides a shortcut menu with the following commands on keystroke records:

- **Copy** (Ctrl+C) - Serves to copy the selected text of the recording to the Clipboard.
- **Select All** (Ctrl+A) - Serves to select the entire text of the keystroke recording.
- **Print** (Ctrl+P) - Serves to print the keystroke recording on the printer.

## Process list

When recording user activity, DeviceLock logs all processes run by the monitored user. The session viewer provides a list of those processes with the following information on each one:


- **Process Name** - The name of the file executed by this process. To view the full path to the file, hover over the file name.
- **Window Title** - The title of the window this process opened. Empty if the process window was hidden. To make the list include such processes, select the **Show hidden processes** option.
- **Start Date/Time** - The date and time that this process started.
- **Finish Date/Time** - The date and time that this process ended. Empty if the process did not end during the monitoring session.
- **Process ID** - The numeric identifier that the operating system assigned to this process during its run.

The place where the process list is displayed depends upon the contents of the session record:







Session contents	List location
Both Video and Keylogger	On the <b>Processes</b> tab in the keystroke recording viewer.
Video only	To the right of the video player.
Keylogger only	To the right of the keystroke recording viewer.

## Managing the UAM Log

The shortcut menu on the **UAM Log Viewer** node provides the following log management commands (next to the command name is the toolbar button corresponding to that command):



- **Settings**  - View or change the settings that limit the maximum number of records the log may contain (see [UAM log settings](#)). This command is provided only for the UAM log on the DeviceLock Enterprise Server.

The **Settings** command is not available for the UAM log on the DeviceLock Service. The log size in this case depends upon the service option [Local storage quota \(%\)](#). For details, see [Local storage quota](#).

- **Refresh**  - Update the list of records with the latest information.
- **Filter**  - Display only the records that match the conditions specified (see [UAM log filter](#)).
- **Quick filters** - Select one of the following options to display only records for a certain period of time:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Send Data to Server**  - Send data from the log to the server/s specified by the [DeviceLock Enterprise Server\(s\)](#) option. Use this command to send the data as soon as possible. Since servers collect log data automatically as it accumulates on the DeviceLock Service, the use of this command is optional.

The **Send Data to Server** command is provided only for the DeviceLock Service's log. This command is not available on the DeviceLock Enterprise Server. To transfer log data between servers, one could use the [log consolidation](#) feature.

These commands are also available in the shortcut menu of each record in the details pane (see [List of Monitoring Sessions](#)).

## Local storage quota

The UAM log on a managed computer depends upon the [Local storage quota \(%\)](#) setting of the DeviceLock Service on that computer. If the quota is exceeded, user activity monitoring rules cease to trigger and new records are not added to the log. A **Local Storage Quota Exceeded** event is logged in the Audit log with the following message: "User Activity Monitor rules are disabled due to insufficient space for local storage directory (%SHADOW\_PATH%)".

If the quota is exceeded while recording user activity, recording stops and the recorded files are saved to the local UAM log. This ensures that the completed portion of the recording is not lost.

When the quota is exceeded, the DeviceLock Service suspends monitoring of user activity until space is freed in the local data storage (for example, by sending logs to the DeviceLock Enterprise Server). Monitoring automatically resumes as soon as there is enough free space in the local data storage.

## UAM log settings

On the DeviceLock Enterprise Server, the dialog box for managing log settings is used to view or change the following parameters:

- **Control log size** - Select this check box to control the number of records in the log and delete outdated records. If this check box is cleared, all available disk space is used to store the log.
- **Keep events for last <number> days** - When this option is selected, the log stores records no older than the number of days specified.
- **Maximum log size: <number> records** - When this option is selected, the log stores no more than the specified number of records. With this option, you must choose the action to perform when the log reaches its maximum size:
  - **Overwrite events as needed** - New records continue to be stored when the maximum log size is reached. Every new record replaces the oldest one in the log.
  - **Overwrite events older than <number> days** - New records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.
  - **Do not overwrite events (clear log manually)** - New records are not added when the maximum log size is reached. To add new records, old ones must be deleted by hand.

To use default settings, click **Restore Defaults**. The default settings are as follows:

- Maximum log size: 10,000 records
- Overwrite events older than 7 days

---

**Note**

- The server deletes old records either by the date indicated in the **Received Date/Time** column (for records received directly from the DeviceLock Service) or by the date indicated in the **Consolidated Date/Time** column (for records received from other servers using [consolidation](#)).
  - If the log has no space for new records and log settings do not allow the deletion of old records, then new records are not added to the log. In this case, when collecting logs from other computers, those records that cannot be added to the log on the server remain on their computers.
- 

## UAM log filter

After applying a filter, the user activity monitor sessions are listed in the console according to the filter settings. To access the settings, use the **Filter** command from the shortcut menu of the UAM log viewer, which opens a dialog box to set, view, or change the filter settings.

Two types of filter are available:

- **Include** - Display only the sessions that match the condition specified. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab and specify conditions on that tab.
- **Exclude** - Do not display the sessions that match the conditions specified. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab and specify conditions on that tab.

The filter can be temporarily disabled by clearing the **Enable filter** check box.

---

**Note**

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

When the filter is enabled, its conditions are defined by entering values in the following fields:

- **Type** - Filter by available types of recording:
  - **Video** - Check box to filter sessions containing only computer screen video recording.
  - **Keylogger** - Check box to filter sessions containing only computer keystrokes recording.

---

**Important**

- If only the **Video** check box is selected, the filter matches only sessions with video recording without keystrokes recording.
  - If only the **Keylogger** check box is selected, the filter matches only sessions with keystrokes recording without video recording.
  - If both check boxes are selected, the filter matches sessions with video and/or keystrokes recording.
-



- **Computer** - The name of the computer on which the monitoring session was recorded. You can use wildcards, as well as specify multiple names separated by semicolons.  
The **Computer** field is only available in the log filter on the DeviceLock Enterprise Server. This field is not available in the log filter on the DeviceLock Service.
- **Rule** - The name of the rule that caused the recording. You can use wildcards, as well as specify multiple rules separated by semicolons.
- **Reason** - Description of the reason of triggering the rule that caused the recording. You can use wildcards, as well as specify multiple reasons separated by semicolons.
- **Duration** - The time span (days, hours, minutes, and seconds) during which recording continued. Possible settings: greater than, less than or equal to the specified value, or in the interval between the specified pair of values.  
The value is entered in the format days:hours:minutes:seconds. Non-significant zeros can be omitted. For example, 00:00:30:00 is equivalent to 30:00, and means 30 minutes.
- **User** - The name of the user whose activity was recorded in the monitoring session. You can use wildcards, as well as specify multiple names separated by semicolons.
- **Server** - The name of the DeviceLock Enterprise Server computer that received the session recording from the DeviceLock Service. You can use wildcards, as well as specify multiple names separated by semicolons.  
The **Server** field is only available in the log filter on the DeviceLock Enterprise Server. This field is not available in the log filter on the DeviceLock Service.
- **Keylogger** - Filtering by data that the user entered from the keyboard during the monitoring session:
  - **Window title** - The title of the application window into which the user typed. You can use wildcards, as well as specify multiple titles separated by semicolons.
  - **Keyboard input** - The words/phrases the user typed. You can use wildcards, as well as specify multiple phrases separated by semicolons.

---

#### Note

- Filtering applies to typed characters only. Filter disregards the names of non-character keys pressed, such as Shift, Alt, Del, Left, Right, End, etc., which are also recorded in the keylog. For example, the `serial number` filter string matches `serial number` as well as `serial [Shift]number` in the keylog.
  - To configure a filter that matches records containing passwords, specify the following mask in the **Keyboard input** field: `*<password>*</password>*`
- 
- **Process name** - The name and path of the executable file of the application into which the user typed. You can use wildcards, as well as specify multiple processes separated by semicolons.
  - **From, To** - The time range settings to filter by record start date and time. These settings are available in the log filter on the DeviceLock Service.
  - **Generated Date/Time** - The time range settings to filter by record start date and time on the DeviceLock Service. These settings are available in the DeviceLock Enterprise Server's log filter.

- **Received Date/Time** - The time range settings to filter records by date and time they were received from the DeviceLock Service. These settings are available in the DeviceLock Enterprise Server's log filter.
- **Consolidation** - The fields to filter by log consolidation-related data (see [Consolidating Logs](#)):
  - **Server** - The name of the remote server from which the record was last received during log consolidation. You can use wildcards, as well as specify multiple names separated by semicolons.
  - **From, To** - The time range settings to filter records by time they were last received from the remote server during log consolidation.

The consolidation-related fields are only available in the log filter on the DeviceLock Enterprise Server. In the log filter on the DeviceLock Service, these fields are not available.

For each time range, the following settings are available:

- **From** - The beginning of the time range. Possible values:
  - **First Record** - Filter starting with the earliest date and time in the respective log field.
  - **Records On** - Filter starting with a particular date and time.
- **To** - The end of the time range. Possible values:
  - **Last Record** - Filter ending with the latest date and time in the respective log field.
  - **Records On** - Filter ending with a particular date and time.

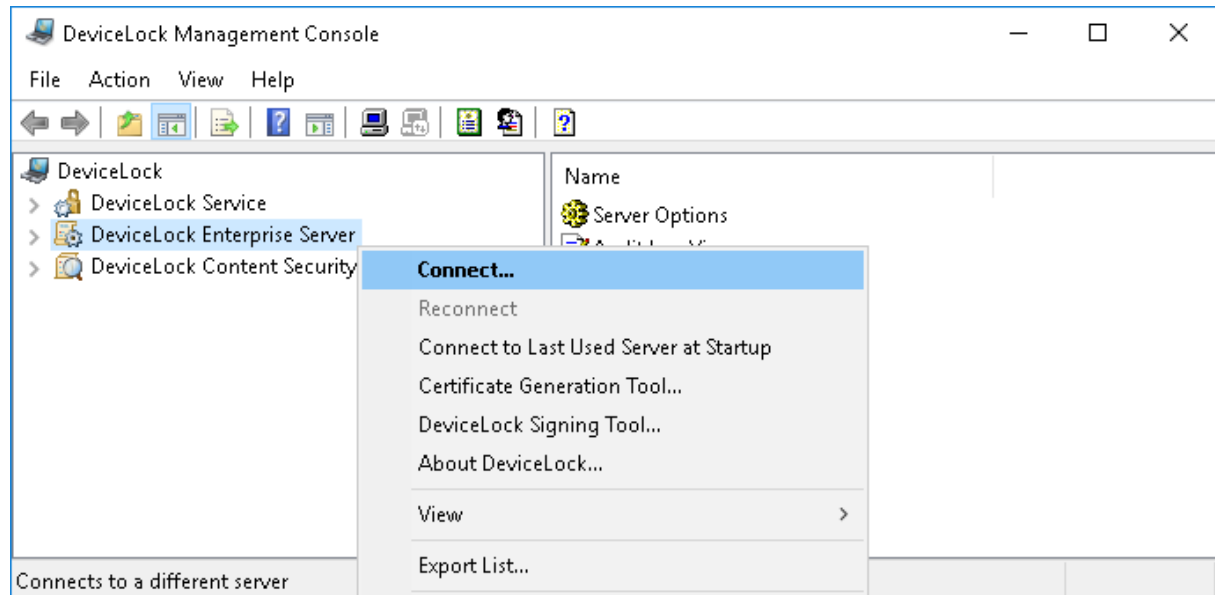
When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given session matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- Filter string fields may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given session matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

# DeviceLock Enterprise Server

## Administering DeviceLock Enterprise Server

Expand the **DeviceLock Enterprise Server** node in the console tree to get access to all of a server's functions and configuration parameters.



The following commands are provided on the shortcut menu available by right-clicking the **DeviceLock Enterprise Server** node:

- **Connect** - Connects to the computer that you specify. For more information, refer to the [Connecting to Computers](#) section of this manual.  
When you connect the console to a computer where an old version of DeviceLock Enterprise Server is installed, you may receive the following message: "The product version on the client and server machines does not match." In this case you need to install the new DeviceLock Enterprise Server version on this computer. For installation instructions, refer to the [Installing DeviceLock Enterprise Server](#) section of this manual.
- **Reconnect** - Connects to the currently connected computer once again.
- **Connect to Last Used Server at Startup** - Check this flag for the DeviceLock Management Console to automatically connect to the last used server each time console starts up.
- **Certificate Generation Tool** - Starts a tool for generating DeviceLock Certificates. See [Generating DeviceLock Certificates](#) for details.
- **DeviceLock Signing Tool** - Starts a tool for granting users temporary access to requested devices and sign DeviceLock Service settings files. See [DeviceLock Signing Tool](#) for details.
- **About DeviceLock** - Displays a dialog box with information about the DeviceLock version and licenses.

## Server Options

These parameters allow you to tune up the DeviceLock Enterprise Server configuration.

	Name	State
DeviceLock		
> DeviceLock Service		
▼ DeviceLock Enterprise Server (screen-e		
> Server Options	Server Administrators	
> Audit Log Viewer	DeviceLock certificate	
> Shadow Log Viewer	Service startup account	.\admin
> UAM Log Viewer	TCP port	Dynamic
> Server Log Viewer	Database name	DeviceLockDB
> Consolidation Servers	Connection type	SQL Server ODBC Driver
> Monitoring	Database server name	screen-e
> Reports	Store path	%SystemRoot%\DLSTORE
> Policies	Store shadow files in the database	Disabled
> Digital Fingerprints	DeviceLock license(s)	Total Windows license(s): 50, Used: 0;
> DeviceLock Content Security Server	Stream compression	Enabled
	Unpack ISO images	Disabled
	Session volume limit for data collection (MB)	1024
	Log consolidation	Not Configured

You can configure the following parameters:

- **Server Administrators** - The list of server administrators and their associated access rights.
- **DeviceLock certificate** - The DeviceLock certificate for DeviceLock Enterprise Server.  
For more information about these parameters, see [Server Administrators](#).
- **Service startup account** - The service account for running for DeviceLock Enterprise Server ("Log on as" parameter).
- **TCP port** - The TCP port for connecting the console to DeviceLock Enterprise Server.  
For more information about these parameters, see [Service account and connection settings](#).
- **Database name** - The name of the DeviceLock Enterprise Server's database.
- **Connection type** - Determines the ODBC driver or system data source to connect to the DeviceLock Enterprise Server's database server.
- **Database server name** - The name of the server that manages the DeviceLock Enterprise Server's database. This setting is available for the ODBC driver connection type.
- **Database server login** - The login to access the DeviceLock Enterprise Server's database. This setting is available if the connection to the database requires a login (such as in the case of SQL Server Authentication mode or when using PostgreSQL as the database server).
- **System data source** - The name of the data source to access the DeviceLock Enterprise Server's database server. This setting is available for the system data source connection type.  
For more information about database-related parameters, see [Database settings](#).
- **Store shadow files in the database** - Where DeviceLock Enterprise Server stores shadow files: in the database or on the disk.
- **Store path** - Where DeviceLock Enterprise Server stores shadow files on the disk.  
For more information about these parameters, see [Store shadow files in the database](#).
- **DeviceLock license(s)** - View DeviceLock license-related information and load your DeviceLock licenses. For details, see [License information](#).

- **Stream compression** - Enable this parameter for DeviceLock to compress audit logs and shadow data when sending it from DeviceLock Service to DeviceLock Enterprise Server. Doing so reduces network load.
- **Unpack ISO images** - Enable this parameter for DeviceLock Enterprise Server to extract files from shadowed CD/DVD/BD images.
- **Session volume limit for data collection (MB)** - Enable this parameter to limit the volume of data gathered from a single computer, which might enhance the overall data collection performance.
- **Log consolidation** - View or change the [log consolidation settings](#). See [Consolidating Logs](#) for details.

The shortcut menu on the **Server Options** node provides the following command:

- **Properties** - Starts the wizard for managing server options.

For further details, see [Managing Server Options](#).

## Server Administrators

The **Server Administrators** node is used to manage the list of server administrators and their rights on DeviceLock Enterprise Server, and to install or remove the DeviceLock certificate for this server.

The shortcut menu on this node provides the following command:

- **Properties** - Opens a dialog box to view or change the list of server administrators, and to install or remove a DeviceLock certificate.

See also:

[Server administrators and certificate](#)

## Managing Server Options

Use the shortcut menu available by a right mouse click, or double-click **Stream compression**, to enable or disable this parameter. By enabling **Stream compression**, you instruct DeviceLock to compress audit logs and shadow data when transmitting them from a DeviceLock Service to the DeviceLock Enterprise Server. Compression decreases the volume of the transferred data, thereby reducing network load.

By enabling the **Unpack ISO images** parameter, you cause the DeviceLock Enterprise Server to extract files from shadowed CD/DVD/BD images. If this parameter is enabled, all files are extracted from CD/DVD/BD images upon delivery to the server and stored in the database separately (one record per file). Otherwise, whole shadowed CD/DVD/BD images are stored in the database.

By enabling the **Session volume limit for data collection (MB)** parameter, you can limit the volume of data gathered from a single computer in order to potentially enhance overall collection performance when gathering data. Enabling this parameter is helpful when a large amount of data gathered from some computers prevents the DeviceLock Enterprise Server from finishing the

procedure for all requests in a reasonable timespan. If this parameter is enabled, the DeviceLock Enterprise Server only gathers the specified amount of data (default value for the parameter is 1024 MB), and then starts gathering data from the next computer request without terminating the previous connection or process.

Use the **Properties** command from the shortcut menu on other parameters to view or change their settings in the dialog box that appears. Alternatively, you can double-click the parameter to open its dialog box.

To run the configuration wizard and review or set parameters step by step, choose the **Properties** command from the shortcut menu on the **Server Options** node. The respective parameter settings and the configuration wizard are described in the sections that cover installation of DeviceLock Enterprise Server (see [Service account and connection settings](#), [Server administrators and certificate](#), [License information](#), [Database settings](#)).

## Using Log Viewers

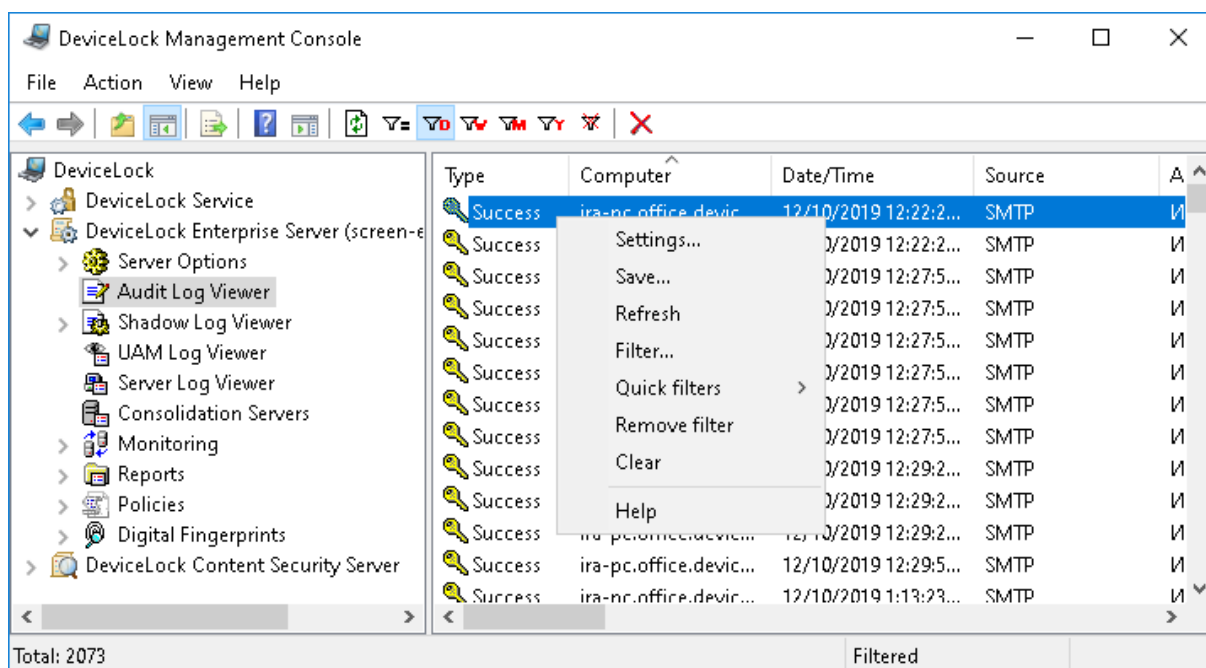
DeviceLock Enterprise Server provides the following tools for viewing DeviceLock logs:

- [Audit Log Viewer \(Server\)](#) - View the audit log stored on the server.
- [Shadow Log Viewer \(Server\)](#) - View the shadow log stored on the server.
- [UAM Log Viewer](#) - View the [User Activity Monitor](#) log stored on the server.
- [Server Log Viewer](#) - View the DeviceLock Enterprise Server's internal log.

### Audit Log Viewer (Server)

The audit log viewer allows you to view the audit log stored on DeviceLock Enterprise Server.

DeviceLock Enterprise Server stores audit records received from a remote computer if **DeviceLock Log** is selected in the [Audit log type](#) parameter in [Service Options](#) on that computer. Otherwise, audit records are stored in the local Windows event logging subsystem of the remote computer, and can be viewed using the service's audit log viewer (see [Audit Log Viewer \(Service\)](#)).



There is not much difference between the service audit log viewer and the server audit log viewer, so first read the [Audit Log Viewer \(Service\)](#) section of this manual.

Compared with the service's audit log viewer, the server's viewer has the following additional columns:

- **Computer** - The name of the computer on which this event was logged by DeviceLock Service.
- **Event** - The ID number of the event.
- **Received Date/Time** - The date and time when DeviceLock Enterprise Server received this event from DeviceLock Service.
- **Server** - The name of the computer running DeviceLock Enterprise Server that received this event from DeviceLock Service.
- **Consolidated Date/Time** - The date and time that this event was last received from the remote server during log consolidation (see [Consolidating Logs](#)).
- **Consolidation Server** - The name of the remote server from which this event was last received during log consolidation (see [Consolidating Logs](#)).

The **Reason**, **Name** and **Information** columns may display additional information about the device, enclosed in brackets. The console retrieves that information from the Description field of the USB Devices database. If no data can be found in the Description field for a given device, the additional information indicates the device's PID, VID, and serial number or system identifier.







## Managing the Audit Log (Server)

The log can be managed by using commands from the shortcut menu:

- In the DeviceLock Management Console tree, expand **DeviceLock Enterprise Server**, and then right-click **Audit Log Viewer** under the **DeviceLock Enterprise Server** node.
- OR -



- In the DeviceLock Management Console tree, select **DeviceLock Enterprise Server > Audit Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings** - View or change the settings that limit the maximum number of event records the log may contain (see [Audit Log Settings \(Server\)](#)).
- **Save** - Save the log to the file you specify.
- **Refresh**  - Update the list of events with the latest information.
- **Filter**  - Display only the events that match the conditions specified (see [Audit Log Filter \(Server\)](#)).
- **Quick filters** - Choose from the following options to view the events that occurred during:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

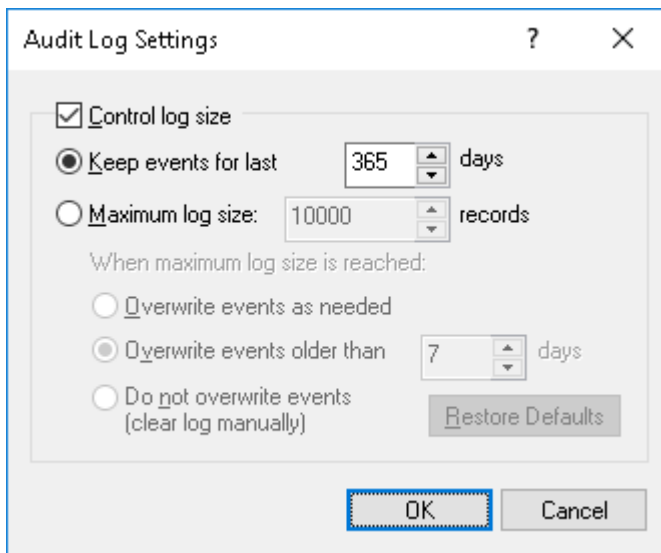
A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Clear**  - Delete all event records that currently exist in the log.  
This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.

## Audit Log Settings (Server)

To control the log size and server actions when the log is overflowing, select the **Settings** command from the shortcut menu of this log viewer in the console tree. Then, view or change the settings in the dialog box that appears.





Select the **Control log size** check box to allow the server to control the number of records in the log and delete outdated records. If this check box is cleared, the server uses all available database space to store the log.

The log size can be controlled by the retention period or number of records:

- **Keep events for last <number> days** - When this option is selected, the log stores records no older than the number of days specified (365 days by default).
- **Maximum log size: <number> records** - When this option is selected, the log stores no more than the specified number of records. In this case, you must select the server action to be performed when the log reaches the maximum size:
  - **Overwrite events as needed** - New event records continue to be stored when the maximum log size is reached. Each record of a new event replaces the oldest record in the log.
  - **Overwrite events older than <number> days** - New event records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.
  - **Do not overwrite events (clear log manually)** - New event records are not added when the maximum log size is reached. To enable the server to add new records, the log must be cleared by hand.

---

#### Note

The server removes old records either by the date indicated in the **Received Date/Time** column (for records received directly from the DeviceLock Service) or by the date indicated in the **Consolidated Date/Time** column (for records received from other servers using [consolidation](#)).

---

To use the default log size, select the option **Maximum log size** and click **Restore Defaults**. The default log size settings are as follows:

- Maximum log size: 10,000 records
- Overwrite events older than 7 days


If the audit log has no space for new records and log settings do not allow the deletion of old records, the server does not remove audit data from users' computers. This prevents the loss of audit data due to lack of space in the log. When some space becomes available in the log, the server moves the remaining audit data from the users' computers to this log.

---

**Note**

- The actual number of event records may temporarily exceed the limit set forth in the log settings, as the cleanup of the log is performed no more than once every 30 minutes to reduce the load on the SQL server.
  - If multiple DeviceLock Enterprise Servers use the same database, then the actual number of event records may slightly exceed the limit set forth in the log settings.
  - The log settings are stored in the database, and are relating to the log rather than to the server. All DeviceLock Enterprise Servers that use the same database have the same log settings.
- 

## Audit Log Filter (Server)

You can filter data in [Audit Log Viewer \(Server\)](#) so that only records that meet specified conditions are displayed in the list. To open the **Filter** dialog box, choose **Filter** from the shortcut menu of **Audit Log Viewer** or click  on the toolbar.

Filter
?
X

☒ Include
☐ Exclude

Event types

☒ Success
☒ Warning
☒ Information
☒ Failure

Computer:
Name:
Source: Service
Action: Keylogger Detected
Information:
Reason:
User:
Process:
PID:
Server:
Event ID:

Generated Date/Time
From: First Event 1/ 1/2020 12:00:00 PM
To: Last Event 1/ 1/2020 12:00:00 PM

Received Date/Time
From: First Event 1/ 1/2020 12:00:00 PM
To: Last Event 1/ 1/2020 12:00:00 PM

Consolidation
Server:
From: First Event 1/ 1/2020 12:00:00 PM
To: Last Event 1/ 1/2020 12:00:00 PM

☒ Enable filter
Clear Load Save

OK Cancel

The server audit log filter is configured in the same way as the service audit log filter described in [Audit Log Filter \(Service\)](#).

To set up a filter, select the **Enable filter** check box on the respective tab depending upon whether to configure include or exclude conditions.

---

**Note**

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

This filter has the same setting fields as the service's audit log filter plus the following fields:

- **Computer** - The name of the computer on which this event was logged by DeviceLock Service. This field is case-insensitive.
- **Server** - The name of the computer running DeviceLock Enterprise Server that received the event from DeviceLock Service. This field is case-insensitive.
- **Event ID** - The ID number of the event. To enter multiple numbers, separate them with a semicolon (;).
- **Generated Date/Time** - The time range settings to filter events by time they were logged by DeviceLock Service.
- **Received Date/Time** - The time range settings to filter events by time when DeviceLock Enterprise Server received them from DeviceLock Service.
- **Consolidation** - The fields to filter by log consolidation-related data (see [Consolidating Logs](#)):
  - **Server** - The name of the remote server from which the event was last received during log consolidation. This field is case-insensitive, and allows the use of wildcards (\* and ?). To enter multiple values, separate them with a semicolon (;).
  - **From, To** - The time range settings to filter events by time they were last received from the remote server during log consolidation.

For each time range, the following settings are available:

- **From** - The beginning of the time range. Possible values:
  - **First Event** - Filter starting with the earliest date and time in the respective log field.
  - **Events On** - Filter starting with a particular date and time.
- **To** - The end of the time range. Possible values:
  - **Last Event** - Filter ending with the latest date and time in the respective log field.
  - **Events On** - Filter ending with a particular date and time.

---

**Note**

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.

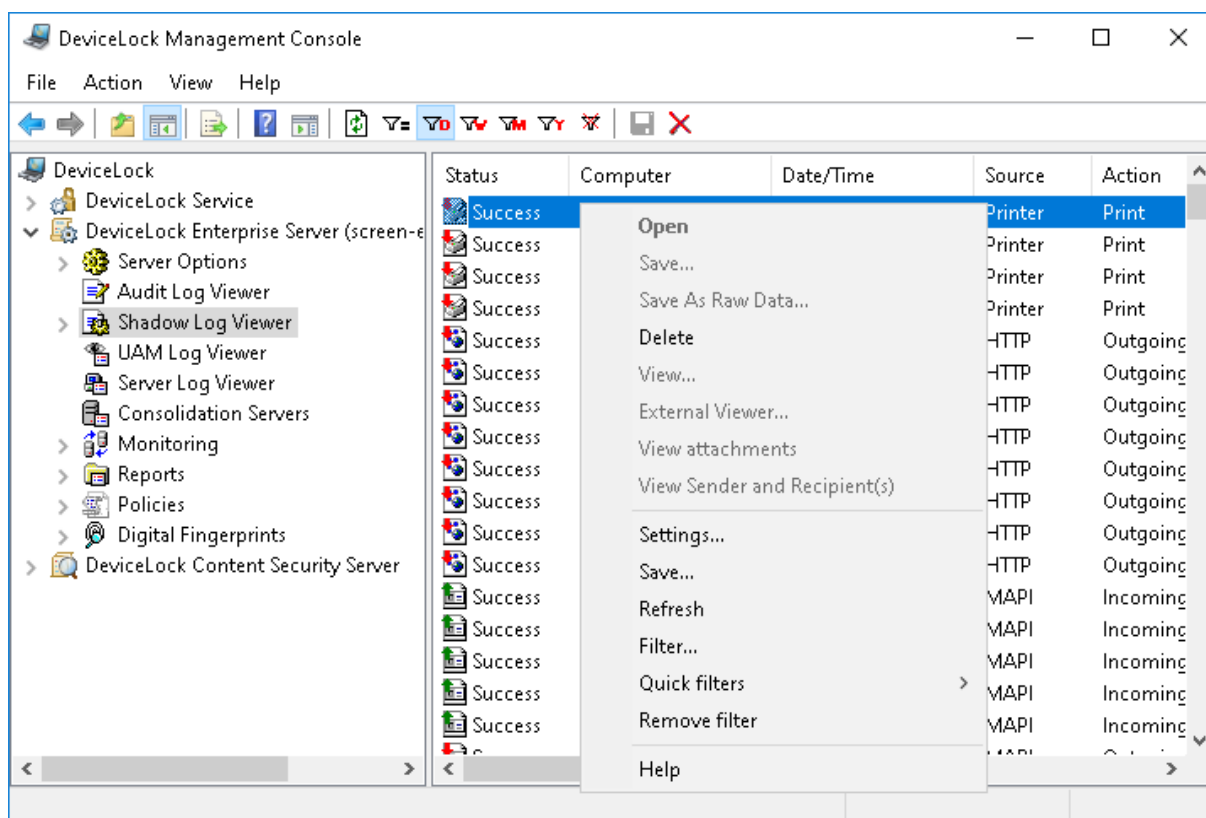
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

When configuring a filter by the **Name**, **Reason** or **Information** field, consider the following:

- The filter is applied to the data shown in the event list columns. Since the **Name**, **Reason** and **Information** columns may include device descriptions, the filter may cause the list to include (or exclude) devices whose description matches the filter condition in the **Name**, **Reason** or **Information** field.
- An event satisfies the filter condition if any part of the **Name**, **Reason** or **Information** column data matches the respective filter field. For example, events with USB device (USB-Admin), USB device (Admin) or USB device (Administrator) in the **Name** column match the filter condition with Admin specified in the **Name** field.
- As applied to device descriptions in the **Name**, **Reason** or **Information** column, wildcards such as \* or ? function as separators in the respective filter fields. An event matches the filter if any part of the column data matches any part of the filter data separated by a wildcard. For example, events with a device description in the **Name** column that includes Admin or User, such as USB device (Administrator) or USB device (USB-User), match filter conditions that have User\*Admin specified in the **Name** field.

## Shadow Log Viewer (Server)

The shadow log viewer allows you to retrieve the shadow log stored on DeviceLock Enterprise Server.



There is not much difference between the service shadow log viewer and the server shadow log viewer, so first read the [Shadow Log Viewer \(Service\)](#) section of this manual.

As compared with the service's shadow log viewer, the server's viewer has the following additional columns:

- **Computer** - The name of the computer on which this event was logged by DeviceLock Service.
- **Received Date/Time** - The date and time that DeviceLock Enterprise Server received this event from DeviceLock Service.
- **Server** - The name of the computer running DeviceLock Enterprise Server that received this event from DeviceLock Service.
- **Consolidated Date/Time** - The date and time that this event was last received from the remote server during log consolidation (see [Consolidating Logs](#)).
- **Consolidation Server** - The name of the remote server from which this event was last received during log consolidation (see [Consolidating Logs](#)).

The **Information** column may display additional information about the device, enclosed in brackets. The console retrieves that information from the Description field of the USB Devices database. If no data can be found in the Description field for a given device, the additional information indicates the device's PID, VID, and serial number or system identifier.

## Managing Shadow Log Records

To manage Shadow Log records, use the shortcut menu available via a right mouse click on every record. The menu includes the following commands:

- [Open](#)
- [Save](#)
- [Save As Raw Data](#)
- [Delete](#)
- [View](#)
- [External Viewer](#)
- [View Attachments](#)
- [View Sender and Recipient\(s\)](#)

Unlike the service's shadow log viewer, when you delete a record in the server's viewer, the record's binary data is removed from the database or from the disk (it depends upon the [Store shadow files in the database](#) flag) but all other information (such as the file name and size, user name, date/time, process and so on) is moved to the special log called [Deleted Shadow Data Log](#).







This Deleted Shadow Data Log is used when you do not need the content of the shadow data anymore and you want to clean up storage (either SQL Server or the disk), but you need to keep information about the data transfer.

## Managing the Shadow Log (Server)

The log can be managed by using commands from the shortcut menu:


- In the DeviceLock Management Console tree, expand **DeviceLock Enterprise Server**, and then right-click **Shadow Log Viewer** under the **DeviceLock Enterprise Server** node.  
- OR -
- In the DeviceLock Management Console tree, select **DeviceLock Enterprise Server > Shadow Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings** - View or change the settings that limit the maximum number of records the log may contain (see [Shadow Log Settings \(Server\)](#)).
- **Save** - Save the log to the file you specify.
- **Refresh**  - Update the list of records with the latest information.
- **Filter**  - Display only the records that match the conditions specified (see [Shadow Log Filter \(Server\)](#)).
- **Quick filters** - Choose from the following options to display only records for a certain period of time:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

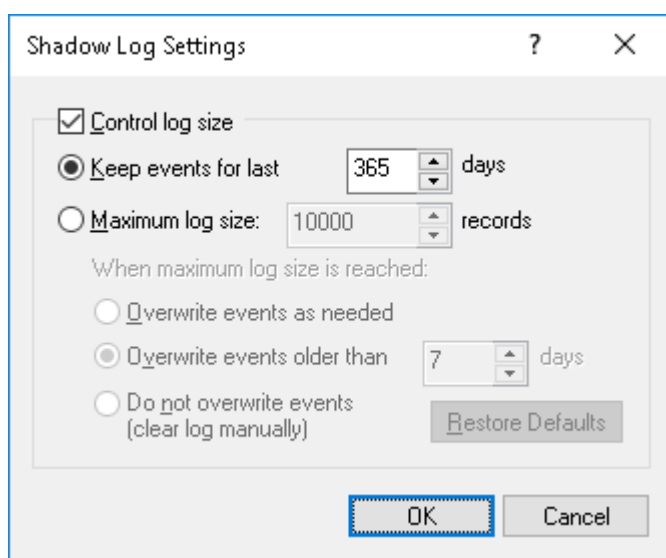
To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.

## Shadow Log Settings (Server)

To control the log size and server actions when the log is overflowing, select the **Settings** command from the shortcut menu of this log viewer in the console tree. Then, view or change the settings in the dialog box that appears.



The log settings are similar to those of the Audit log, see [Audit Log Settings \(Server\)](#).

When DeviceLock Enterprise Server needs to remove old records from the Shadow log because of the log settings specified, those records are moved to the [Deleted Shadow Data Log](#).

---

### Note

The server removes old records either by the date indicated in the **Received Date/Time** column (for records received directly from the DeviceLock Service) or by the date indicated in the **Consolidated Date/Time** column (for records received from other servers using [consolidation](#)).

---

If the Shadow log has no space for new records and log settings do not allow the deletion of old records, the server does not remove shadow data from users' computers. This prevents the loss of shadow data due to lack of space in the log. When some space becomes available in the log, the server moves the remaining shadow data from the users' computers to this log.


It is a best practice to avoid the accumulating of shadow data on users' computers. We recommend that you monitor the server log of DeviceLock Enterprise Server by using the [Server Log Viewer](#) on a



regular basis, watch for warning messages, and appropriately adjust the shadow log settings on the server.

## Shadow Log Filter (Server)

You can filter data in [Shadow Log Viewer \(Server\)](#) so that only records that meet specified conditions are displayed in the list.

To open the **Filter** dialog box, choose **Filter** from the shortcut menu of **Shadow Log Viewer** or click  on the toolbar.

Filter
?
X

☒ Include
☐ Exclude

Shadow status

☒ Success
☒ Incomplete
☒ Failed

Computer:

File name:

\*database\*

Source:

Removable

Action:

User:

\*\Guest

Process:
PID:

Reason:

Server:

Protected:

Information:

File type:

File size

Between
and

80000

bytes

Generated date/time

From:

First Record

1/ 1/2020 12:00:00 PM

To:

Last Record

1/ 1/2020 12:00:00 PM

Received date/time

From:

First Record

1/ 1/2020 12:00:00 PM

To:

Last Record

1/ 1/2020 12:00:00 PM

Consolidation

Server:

From:

First Record

1/ 1/2020 12:00:00 PM

To:

Last Record

1/ 1/2020 12:00:00 PM

☒ Enable filter

Clear
Load
Save

OK

Cancel

The server shadow log filter is configured in the same way as the service shadow log filter described in [Shadow Log Filter \(Service\)](#).

To set up a filter, select the **Enable filter** check box on the respective tab depending upon whether to configure include or exclude conditions.

---

**Note**

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

This filter has the same setting fields as the service's shadow log filter plus the following fields:

- **Computer** - The name of the computer on which this event was logged by DeviceLock Service. This field is case-insensitive.
- **Server** - The name of the computer running DeviceLock Enterprise Server that received this event from DeviceLock Service. This field is case-insensitive.
- **Generated Date/Time** - The time range settings to filter events by time they were logged by DeviceLock Service.
- **Received Date/Time** - The time range settings to filter events by time that DeviceLock Enterprise Server received them from DeviceLock Service.
- **Consolidation** - The fields to filter by log consolidation-related data (see [Consolidating Logs](#)):
  - **Server** - The name of the remote server from which the event was last received during log consolidation. This field is case-insensitive, and allows the use of wildcards (\* and ?). To enter multiple values, separate them with a semicolon (;).
  - **From, To** - The time range settings to filter events by time they were last received from the remote server during log consolidation.

For each time range, the following settings are available:

- **From** - The beginning of the time range. Possible values:
  - **First Record** - Filter starting with the earliest date and time in the respective log field.
  - **Records On** - Filter starting with a particular date and time.
- **To** - The end of the time range. Possible values:
  - **Last Record** - Filter ending with the latest date and time in the respective log field.
  - **Records On** - Filter ending with a particular date and time.

---

**Note**

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

When configuring a filter, consider the following:

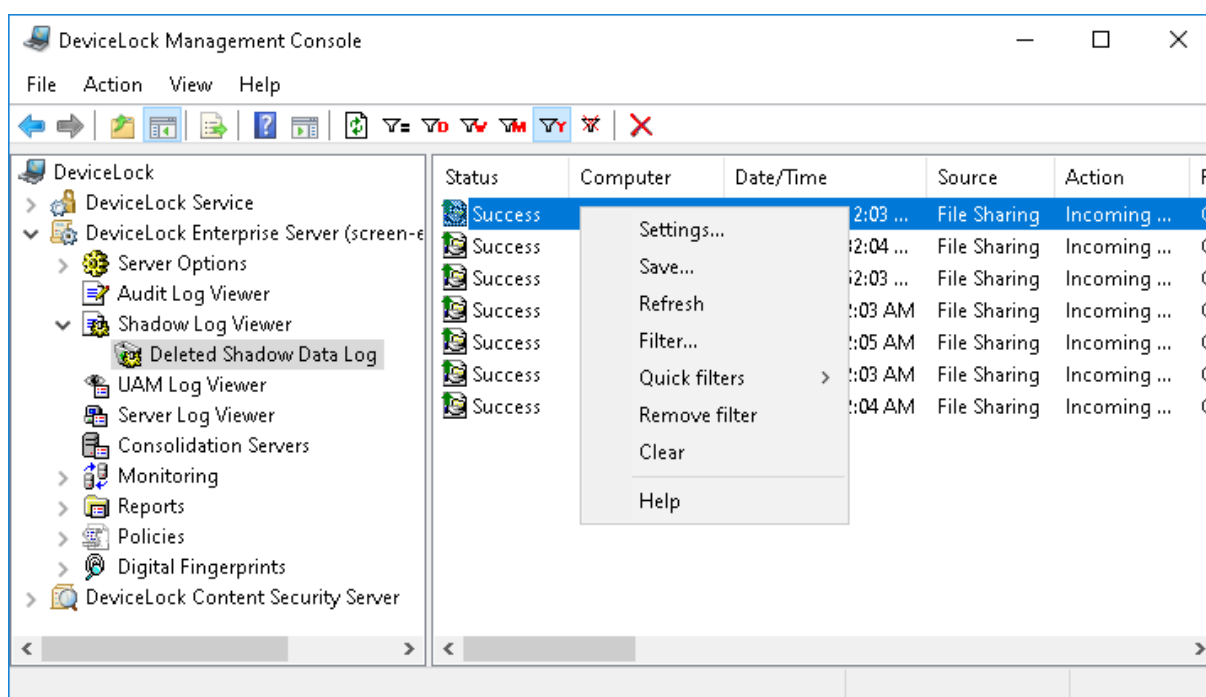
- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.

- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

## Deleted Shadow Data Log

This viewer allows you to retrieve information about deleted shadow log records.

When a record is removed from the shadow log, the record's binary data is deleted but meta-data (such as the file name and size, user name, date/time, process and so on) is moved to this log. The viewer of this log has the same columns as [Shadow Log Viewer \(Server\)](#).



This log is used when you do not need the content of the shadow data anymore and you want to clean up the storage (either SQL Server or the disk) but at the same time you need to keep the information about the data transfer.

The viewer of this log has the same columns as [Shadow Log Viewer \(Server\)](#).

## Managing the Deleted Shadow Data Log

The log can be managed by using commands from the shortcut menu:

- In the DeviceLock Management Console tree, expand **DeviceLock Enterprise Server > Shadow Log Viewer** and then right-click **Deleted Shadow Data Log**.
- OR -

- In the DeviceLock Management Console tree, select **DeviceLock Enterprise Server > Shadow Log Viewer > Deleted Shadow Data Log**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings** - View or change the settings that limit the maximum number of records the log may contain.







The log settings are similar to those of the Audit log, see [Audit Log Settings \(Server\)](#).

---

### Important



If the deleted shadow data log has no space for new records and log settings do not allow the deletion of old records, DeviceLock Enterprise Server just drops the new records. To avoid the loss of records in this way, monitor the server log of DeviceLock Enterprise Server by using the [Server Log Viewer](#) on a regular basis, watch for warning messages there, and appropriately adjust the deleted shadow data log settings.

---

- **Save** - Save the log to the file you specify.
- **Refresh**  - Update the list of records with the latest information.
- **Filter**  - Display only the records that match the conditions specified.  
The filter settings are similar to those of the Shadow log, see [Shadow Log Filter \(Server\)](#).
- **Quick filters** - Choose from the following options to display only records for a certain period of time:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

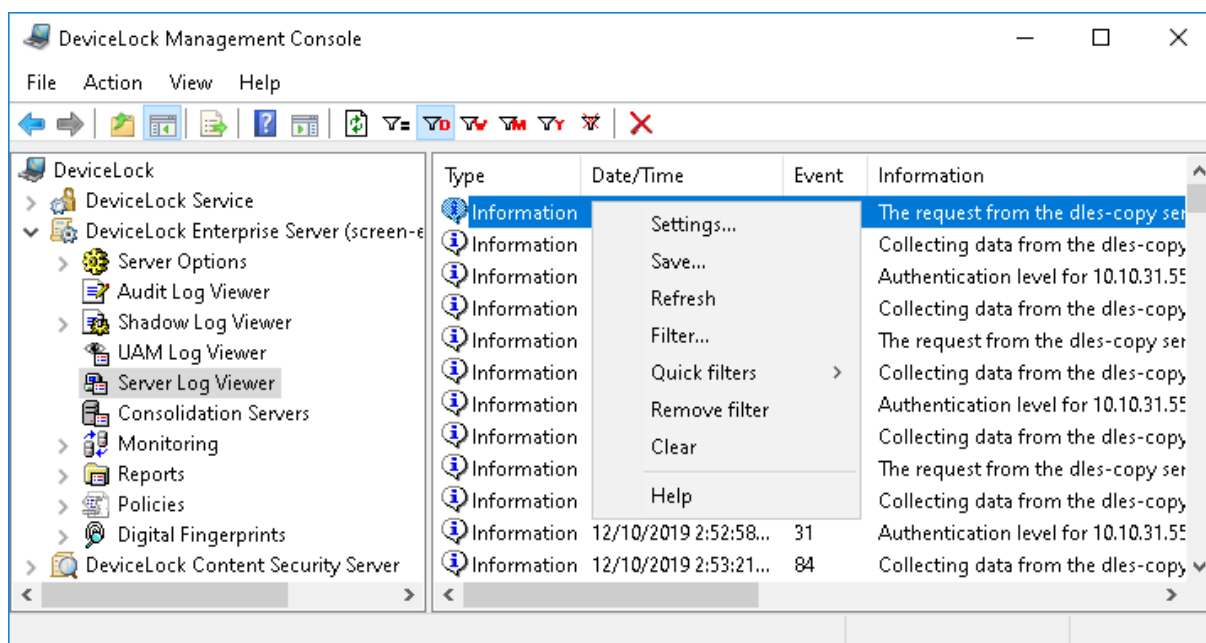
A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Clear**  - Delete all event records that currently exist in the log.

This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.

## Server Log Viewer

This viewer allows you to retrieve the internal DeviceLock Enterprise Server's log. The server uses this log to write errors, warnings and other important information (such as configuration changes, start/stop events, version, and so on).



You may use the information from this log to diagnose problems (if any), to keep track of changes in the server's configuration and to see who has cleared logs and when.

The columns of this viewer are defined as follows:

- **Type** - The event type can be one of the following:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Date/Time** - The date and time that the event occurred.
- **Event** - The ID number of the event.
- **Information** - Event-specific information, such as error/warning descriptions, names and values of changed parameters, and so on.
- **Server** - The name of the computer running DeviceLock Enterprise Server on which this event occurred.
- **Record N** - Sequence number of the event record in the list.
- **Consolidation Server** - The name of the remote server from which this event was last received during log consolidation (see [Consolidating Logs](#)).
- **Consolidated Date/Time** - The date and time that this event was last received from the remote server during log consolidation (see [Consolidating Logs](#)).

## Managing the Server Log







The log can be managed by using commands from the shortcut menu:

- In the DeviceLock Management Console tree, expand **DeviceLock Enterprise Server**, and then right-click **Server Log Viewer** under the **DeviceLock Enterprise Server** node.

- OR -



- In the DeviceLock Management Console tree, select **DeviceLock Enterprise Server > Server Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings** - View or change the settings that limit the maximum number of event records the log may contain (see [Server Log Settings](#)).
- **Save** - Save the log to the file you specify.
- **Refresh**  - Update the list of events with the latest information.
- **Filter**  - Display only the events that match the conditions specified (see [Server Log Filter](#)).
- **Quick filters** - Choose from the following options to view the events that occurred during:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

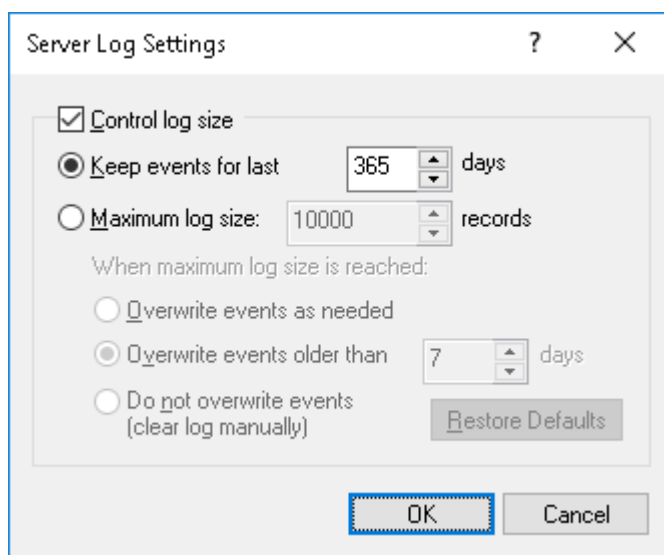
A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Clear**  - Delete all event records that currently exist in the log.

This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.

## Server Log Settings

To control the log size and server actions when the log is overflowing, select the **Settings** command from the shortcut menu of this log viewer in the console tree. Then, view or change the settings in the dialog box that appears.



The log settings are similar to those of the Audit log, see [Audit Log Settings \(Server\)](#).


---

**Note**

The server removes old records either by the date indicated in the **Date/Time** column (for records logged by the local server) or by the date indicated in the **Consolidated Date/Time** column (for records received from other servers using [consolidation](#)).

---

## Server Log Filter

You can filter data in the [Server Log Viewer](#) so that only records that meet specified conditions are displayed in the list. To open the **Filter** dialog box, choose **Filter** from the shortcut menu on **Server Log Viewer** or click  on the toolbar.



The server log filter is configured in the same way as the audit log filter described in [Audit Log Filter \(Service\)](#).

To set up a filter, select the **Enable filter** check box on the respective tab depending upon whether to configure include or exclude conditions.

### Note

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

When the filter is enabled, you can define its condition by entering values into the following fields:

- **Event types** - Select check boxes to filter events by type:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- String fields intended to include or exclude event records depending upon whether event data matches the filter string specified. For example, to filter records by the name of the server on which the event occurred, specify a filter string in the **Server** field. To filter records with certain

event IDs, enter ID numbers separated by a semicolon in the **Event ID** field.

The following string fields are available:

- **Information** - Event-specific information, such as error/warning descriptions, names and values of changed parameters, and so on.
- **Server** - The name of the computer running DeviceLock Enterprise Server on which the event occurred.
- **Event ID** - The ID number of the event.
- **From, To** - The time range settings to filter events by time they were logged by the server.
- **Consolidation** - The fields to filter by log consolidation-related data (see [Consolidating Logs](#)):
  - **Server** - The name of the remote server from which the event was collected during log consolidation. This field is case-insensitive, and allows the use of wildcards (\* and ?). To enter multiple values, separate them with a semicolon (;).
  - **From, To** - The time range settings to filter events by time they were last received from the remote server during log consolidation.

For each time range, the following settings are available:

- **From** - The beginning of the time range. Possible values:
  - **First Record** - Filter starting with the earliest date and time in the respective log field.
  - **Records On** - Filter starting with a particular date and time.
- **To** - The end of the time range. Possible values:
  - **Last Record** - Filter ending with the latest date and time in the respective log field.
  - **Records On** - Filter ending with a particular date and time.

---

### Note

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

## Consolidating Logs

For the sake of load balancing, performance, and fault tolerance, large organizations often deploy multiple instances of the DeviceLock Enterprise Server to gather data from the endpoints' DeviceLock Service logs. Unless each DeviceLock Enterprise Server instance's configuration is pointing to a common back end SQL database, the activity data relating to different users or computers would be stored on different servers. Such distributed data storage can delay investigations and reporting when a complete data set is required for all users and computers. Where having a common back end SQL database the instances can push to is not possible or practical, the issue of having multiple standalone DeviceLock Enterprise Server and database instances can be addressed by DeviceLock's ability to forward the log data from the separate servers to a "central collection server" to consolidate the logs.

This "central collection" DeviceLock Enterprise Server can be used as a central storage for DeviceLock logs from other servers, which are referred to as "remote servers". Remote servers can send copies of their logs to the central collection server on a scheduled basis. Configuration options allow the selection of which logs to send, and when. The central collection server can be located on an on-premises computer or in the cloud (see [Appendix: Consolidating the Logs in the Cloud Using OpenVPN](#)).

The consolidation of logs enables the implementation of a data/traffic management scenario where the remote servers accumulate logs during working hours, and at night they forward the accumulated data to the central collection server. For example, organizations with branches across multiple geographic areas could deploy servers in their branch offices to collect locally during work hours and then forward logs to a central collection server after hours. The main advantage of such a deployment is that the collection and forwarding of logs do not overload communication channels between branches during normal working hours. At night, when the channels are mostly idle, it would be practical to forward the remote server log data to the central collection server. As a result, the central server collects logs from all branches without any adverse effect on network communication channels, and the full log data set would be available for investigation and reporting purposes each morning.

For further details, see [Getting Started Using the Consolidation of Logs](#).

## Getting Started Using the Consolidation of Logs

To use the consolidation of logs, an administrator of DeviceLock Enterprise Server first needs to decide which server will be used as the central collection server, and then configure other, remote servers to forward logs to that server.

On every server that is intended to forward logs to the central collection server, the administrator has to configure the [log consolidation settings](#) by specifying:

- The name of the computer running the central collection DeviceLock Enterprise Server.
- The schedule of sending logs to the central collection server.

- Which logs to send to the central collection server.
- Whether to copy or move log data (in the latter case, the data will be deleted from the remote server).
- Whether to limit the network bandwidth utilization for transmitting log data to the central collection server.

When configuring log consolidation, the administrator must also specify the way of authentication between the remote server/s and central collection server. The following authentication options are available:

- Certificate (recommended option, see [DeviceLock Certificates](#)) - The private key of the certificate must be installed on the central collection server by using the "DeviceLock certificate" parameter in [Server Options](#). The public key of that certificate must be supplied along with the name of the central collection server in the log consolidation settings on the remote server/s. Another option is to install the private key of the central collection server's certificate on the remote server/s by using the "DeviceLock certificate" parameter in [Server Options](#). In this case, the public key on the remote server is not required.
- Windows account - The Windows service "DeviceLock Enterprise Server" on the central collection server must be running under an account with DeviceLock Enterprise Server administrator rights on the remote server/s.

To view all remote servers that forward their logs to the central server, use the DeviceLock Enterprise Server > [Consolidation Servers](#) list in the console connected to the central collection server. This list shows the names of the remote servers, the schedule for sending logs to the central server, the current status of each server, as well as the amount of data transferred to the central collection server.

## Administering the Consolidation of Logs

The administrator can configure DeviceLock Enterprise Server to consolidate DeviceLock logs on the central collection server. DeviceLock Management Console provides the following controls for this:

- [Log consolidation settings](#) - On the remote server/s, view or change the central collection server connection settings such as the server name, authentication options, log selection and sending schedule and other options.
- [Consolidation server list](#) - On the central collection server, view details of the remote servers forwarding their logs to this server, including server names, log transfer status and schedule, and volumes of data transferred and awaiting transfer.

### Log consolidation settings

To configure DeviceLock Enterprise Server as a remote server that would be forwarding its logs to the central collection server, use the **Log consolidation** parameter in **DeviceLock Enterprise Server > Server Options** in the DeviceLock Management Console connected to the remote server. The **Properties** command on this parameter opens a dialog box with the following settings:

- **Consolidation server** - The name or IP address of the computer running the central collection DeviceLock Enterprise Server. Only one computer can be specified in this field.
- **Set Credentials** - Opens a dialog box to configure authentication between the remote server and central collection server. For details, see [Configuring authentication](#).
- **Schedule** - The following options are used to configure the schedule of sending logs from this server to the central collection server:
  - **Hourly** - Choose the date and time to start sending the logs and the recurrence interval. For example, an interval of 1 produces an hourly schedule and an interval of 2 produces an every-other-hour schedule. The remote server will send the logs each hour.
  - **Daily** - Choose the date and time to start sending the logs and the recurrence interval. For example, an interval of 1 produces a daily schedule and an interval of 2 produces an every-other-day schedule. The remote server will send the logs at the specified time each day.
  - **Weekly** - Choose the date and time to start sending the logs, the days of the week on which to send the logs, and the recurrence interval. For example, an interval of 1 produces a weekly schedule and an interval of 2 produces an every-other-week schedule. The remote server will send the logs at the specified time on each of the specified days.
  - **Monthly** - Choose the months in which to send the logs and the weeks of the month and the days of the week for each month in which to send the logs. This option can also be configured to send the logs on a certain last day of each month.
- **Stop data transfer after <number> hours / days** - When this check box is selected, the transfer of the logs stops in the lapse of the specified time after it starts, even if the remote server did not manage to transfer all the log data it has. Data that has not been transferred is stored on the remote server for sending during the next scheduled transfer of logs.
- **Logs** - Select the check box next to the name of each of the logs to transfer to the central collection server. The remote server will forward only the selected logs.
- **Consolidation Mode** - The following options specify whether consolidation moves or just copies log data:
  - **Full** - The log records transferred to the central collection server are deleted from the remote server. The Shadow log records are permanently deleted, without retaining their copies in the Deleted Shadow Data log on the remote server.
  - **Copy** - The log records transferred to the central collection server remain in the logs on the remote server.
    - **File names only** - This check box only affects the transfer of shadow copy data. When this check box is selected, file names are transferred from the Shadow log to the central collection server, and the files themselves and other shadow copy data remain only on the remote server.


---

## Note

- Switching synchronization mode from **Copy** to **Full** deletes from the remote server the log records that were earlier copied to the central collection server.
  - When switching synchronization mode from **Copy | File names only** to **Full**, the missing files and data are copied to the central collection server and then those files and data are deleted from the remote server.
- 
- **Traffic Priority** - The following options specify whether to limit the network bandwidth utilization for transmitting log data to the central collection server:
    - **High** - Do not limit the utilization of the network bandwidth.
    - **Medium** - Utilize at most 50% of the network bandwidth.
    - **Low** - Utilize at most 20% of the network bandwidth.
  - **Advanced Settings** - Opens a dialog box to configure retries of data exchange in case of failure in the communication channel between the consolidation servers. For details, see [Retry parameters](#).
  - **Test Connection** - Click this button to check if the remote server with the current settings can establish a connection to the central collection server. If the connection fails, an error message appears describing the cause of the failure. Otherwise, a message box appears indicating the connection is successfully established.

## Configuring authentication

When you click **Set Credentials** in the dialog box for log consolidation settings, the console opens a dialog box to view, set or change parameters of authentication between the remote server and central collection server:

- **Certificate name** - The public key of the DeviceLock certificate (see [DeviceLock Certificates](#)) for central collection server authentication. The private key of that certificate must be installed on the central collection server by using the "DeviceLock certificate" parameter in [Server Options](#). The public key can be supplied in the dialog box that appears when you click the  button next to the **Certificate name** field. The **Remove** button allows you to delete the public key from the remote server.

Supplying the public key is not required if any of the following conditions is met:

- The Windows service "DeviceLock Enterprise Server" on the central collection server is running under an account with DeviceLock Enterprise Server administrator rights on the remote server.
- The private key of the same certificate is installed on both the central collection server and remote server by using the "DeviceLock certificate" parameter in [Server Options](#).

## Retry parameters

When you click **Advanced Settings** in the dialog box for log consolidation settings, the console opens a dialog box to view, set, or change parameters of retries of data exchange in case of failure

in the communication channel between the consolidation servers:

- **Number of retries** - Specifies the maximum number of times to retry data exchange in a situation where the remote server cannot reach the central collection server or the central server fails to collect logs from the remote server. If this parameter is set to 0, no retries of data exchange are performed.
- **Retry timeout** - Specifies the time interval between successive attempts to exchange data between the servers. In the event of a communication failure, the server waits the specified number of seconds before attempting to communicate again.

Different remote servers may have different retry parameters. The remote server employs its retry parameters when issuing a consolidation request to the central collection server. If the request is successful, the same parameters are then used by the central server when collecting logs from the respective remote server.

When configuring retry parameters, consider how data exchange retries are related to the regular log collection on a schedule:

- The retry count is reset only upon successful data exchange. If the specified number of retries were made and all of them were not successful, then, until the logs are successfully submitted to the central collection server, attempts of their transmission occur only on a schedule, without retries in case of communication failure between the servers. Retries can be resumed only after the logs are successfully collected.
- The regular log collection on a schedule takes precedence over retries. When a retry is scheduled on a later time than the start of a regular log collection session, the session will start according to the schedule, regardless of the scheduled retry. In this case, if the session fails, the retry will occur on the lapse of the retry timeout after session start.

## Consolidation server list

The servers that claimed themselves as remote servers to a given central collection instance of DeviceLock Enterprise Server, are listed in the DeviceLock Management Console connected to that central instance. The list appears in the details pane when you select **DeviceLock Enterprise Server > Consolidation Servers** in the console tree, and it provides the following details of each remote server:

- **Name** - The name of the computer running the remote server.
- **Status** - One of the following:
  - **Uploading** - Logs are currently being transferred from this server to the central collection server.
  - **Finished** - Logs from this server have been successfully transferred to the central collection server.
  - **No license** - The central server cannot collect audit and/or shadow logs from this server due to lack of licenses. To successfully consolidate logs, the number of licenses on the central collection server must be no less than the total number of client computers that forward their logs to the remote servers.

- **Off Schedule** - The central collection server was unable to contact this server at the scheduled date and time of the log transfer.
- **Error** - The central server was unable to collect logs from this server due to an error.

---

#### Note

**Off Schedule** or **Error** status indicates a failure transferring logs from the remote server. The date and time of the last successful transfer are displayed in the **Last Session** column. Additional information on the cause of the failure can be found in the error event logged on the remote server and/or central collection server (see [Server Log Viewer](#)).

---

- **Schedule** - The next scheduled date and time of the log transfer by this remote server.
  - **Last Session** - The date and time that the last log transfer session was completed by this remote server.
  - **Received Data** - The total amount of data the central server received from this remote server for the whole time.
  - **Session Data** - The amount of data the central server received from this remote server in the current/last completed log transfer session.
  - **Remaining Data** - The amount of remaining data the central server expects to receive from this remote server.
- 

#### Note

Information about the data amounts is updated at the beginning of the log transfer session, during the session, and at the end of the session. Between sessions, information is displayed as of the end of the last completed log transfer session.

---

The shortcut menu on each of the listed remote servers provides the following commands:

- **Connect to DeviceLock Enterprise Server** - Connects the console to the given remote server.
- **Log Consolidation Settings** - Opens the dialog box to view or change the [log consolidation settings](#) on the given remote server.
- **Refresh** - Updates the list of remote servers with the most recent information.
- **Remove** - Hides the selected server in the list. All log data previously collected from this server remains on the central collection server. Should such a “hidden” server present new data for consolidation, it will appear in the list again.

For further details, see [Consolidating Logs](#).

## Monitoring

The monitoring function of DeviceLock Enterprise Server allows you to implement real-time monitoring of DeviceLock Services across the network. DeviceLock Enterprise Server can monitor remote computers in real-time, checking DeviceLock Service status (running or not), policy consistency and integrity. The detailed information is written to the special log and can be viewed using the [Monitoring Log Viewer](#).



Also, it is possible to define a master policy that can be automatically applied across selected remote computers in the event that their current policies are suspected to be out-of-date or damaged.

With DeviceLock Enterprise Server's monitoring function, it is possible to distribute DeviceLock Service to client computers, which allows for an additional way to deploy DeviceLock Service beyond the traditional methods (software installation GPO, Microsoft SCCM, DeviceLock consoles, local Setup, etc.). For more information, see [Installation via DeviceLock Enterprise Server](#).

Moreover, you can use this policy recovery feature as an alternative way of deploying settings, permissions, audit, shadowing rules and alerts to remote DeviceLock Services across the network.

All monitoring-related actions are performed by tasks. The tasks are listed in the details pane when you select the **Monitoring** node in the console tree. Task management includes:

- Creating a new task - Right-click the **Monitoring** node and select **Create Task**.
- Editing an existing task - Select the **Monitoring** node, right-click the task in the details pane, and select **Edit Task**.
- Managing the computer list for an existing task - Right-click the task and select **Edit Computers List**. This command is displayed only if the task has a static list of computers. For further details, see [Create/Edit Task](#).
- Immediately running a task - Right-click the task and select **Run Now**.
- Viewing computers monitored by a particular task - Expand the **Monitoring** node and select the task in the console tree. The list of computers appears in the details pane. For details, see [Task and Its Monitored Computers](#).

You can connect the console to the DeviceLock Service on a monitored computer: right-click the computer in the list and select **Connect to DeviceLock Service**.

- Deleting a task - Right-click the task and select **Delete Task**.

## Monitoring Tasks

The monitoring-related actions are performed by tasks. On a single DeviceLock Enterprise Server, you can have as many tasks as you wish. The maximum number of tasks on one server is only limited by available memory, CPU and network's bandwidth capacity. Please keep in mind that the server should have enough resources to communicate with at least 10 remote computers simultaneously.

By default, DeviceLock Enterprise Server can execute up to 30 tasks simultaneously. This means that if you have, for example, 40 tasks and all of them run at the same time, the first 30 tasks will run first and each of the remaining 10 tasks will run as soon as others complete.

However, you can change the number of tasks that can be run simultaneously by modifying the registry. To define the new number, add the following registry value on the computer running DeviceLock Enterprise Server:

- Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer
- Value: ConcurrentJobs=dword:<number\_of\_threads>

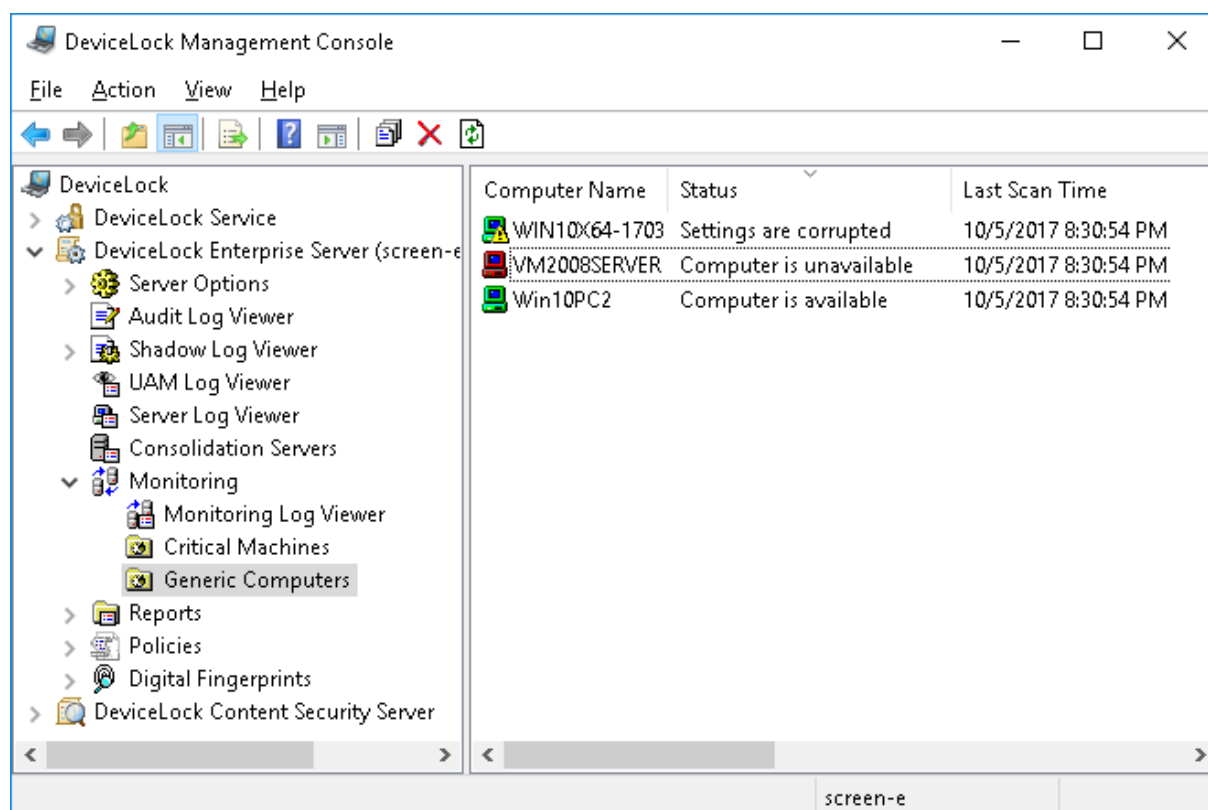
In this value, <number\_of\_threads> must be an integer from 1 to 1000.

During their execution, tasks write status information to the monitoring log (see [Monitoring Log Viewer](#)) including data about monitored computers and DeviceLock Services. They'll also write possible errors which occurred during the scanning of computers and connecting to DeviceLock Services.

Also, tasks display the status of monitored computers and other useful information at the management console. This allows you to keep an eye on monitored computers in real-time.

## Task and Its Monitored Computers

The console displays monitoring tasks in the console tree under **DeviceLock Enterprise Server > Monitoring > Tasks**.



When you select a monitoring task in the console tree, the details pane lists the computers monitored by that task. To update the information displayed in the computer lists, right-click the task and select **Refresh**.

The computer list provides the following information on each computer:

- **Computer Name** - The name of the monitored computer.
- **Status** - The status of the monitored computer and DeviceLock Service.  
The status also affects the small picture (an icon) displayed next to the **Computer Name** parameter. The general rules for interpreting computer icons are as follows:
  - Green computer - The computer is working and DeviceLock Service is running on it.
  - Red computer - The computer is not working/not found, or it is working but without DeviceLock Service.

- Computer with exclamation point - Something is wrong with the computer or DeviceLock Service.

There can be eight different statuses:

- **Computer is available** - The monitored computer is working and DeviceLock Service is running on it. Also, if this task verifies policy integrity, then verification happened without any errors. The computer's icon will be "green computer".  
*If this task restores the broken policy, the computer's icon will be "green computer with exclamation point".*
- **Computer is unavailable** - The DeviceLock Enterprise Server is unable to scan the monitored computer. This occurs when a computer is not working or connections are blocked by a firewall, but the computer's name/address can be resolved through DNS. The computer's icon will be "red computer".
- **Service is unavailable** - The DeviceLock Enterprise Server is unable to connect to DeviceLock Service on the monitored computer. This occurs when the computer is working but DeviceLock Service is not running. Also, it could be the result of running DeviceLock Service on a different TCP port than that specified in the task configuration or due to connections being blocked by the firewall. The computer's icon will be "red computer with exclamation point". For more information on connection issues, see the [Service connection settings](#) parameter description.
- **Settings are corrupted** - The monitored computer is working and DeviceLock Service is running on it but some of the DeviceLock Service settings on that computer differ from the master policy assigned to the monitoring task (see the [Verify Service Settings](#) parameter description). The computer's icon will be "green computer with exclamation point".  
Right-click the computer and select **View details** from the shortcut menu to review the DeviceLock Service settings on the monitored computer that do not match the master policy. The **View details** command brings up a dialog box that lists the non-matching settings, with each setting followed by a description of the mismatch, such as:
  - **non-existent** - The setting is specified in the master policy, but is missing from the monitored computer.
  - **changed** - The setting is specified differently in the master policy and on the monitored computer.
  - **excessive** - The setting is marked as deleted in the master policy, but is specified on the monitored computer.
- **Unresolved computer address** - The DeviceLock Enterprise Server is unable to resolve the name/address of the computer. This happens when an invalid computer name that does not exist in DNS is specified. Also, it could happen because there is no DNS server. In this case the **Unresolved computer address** status should be treated as **Computer is unavailable**. The computer's icon will be "red computer with exclamation point".
- **Unsupported service version** - The DeviceLock Enterprise Server is trying to download a policy (service settings) from DeviceLock Service version 6.2 and lower. The policy verification is supported only for version 6.2.1 and later. The computer's icon will be "green computer with exclamation point".

- **Access is denied** - The DeviceLock Enterprise Server is unable to connect to DeviceLock Service due to lack of privileges. It happens when the account under which the DeviceLock Enterprise Server service starts has no rights to connect to DeviceLock Service. The computer's icon will be "green computer with exclamation point". For information on how to resolve this issue, see the [Service connection settings](#) parameter description.
- **No License** - The DeviceLock Enterprise Server is unable to monitor the computer running DeviceLock Service due to an insufficient number of licenses. DeviceLock Enterprise Server handles as many DeviceLock Service instances as there are licenses loaded into DeviceLock Enterprise Server. For more information, see [License information](#) in [Installing DeviceLock Enterprise Server](#). The computer's icon will be "green computer with exclamation point".

Also, the status messages (except **Computer is available**) are written to the monitoring log (see [Monitoring Log Viewer](#)) so you can view the status of each monitored computer later.

- **Last Scan Time** - The date and time of the last scan attempt. This scan attempt can be either successful or not.
- **Last Successful Scan Time** - The date and time of the last successful scan attempt.
- **Service Uptime** - Shows how long DeviceLock Service has been working on the monitored computer.
- **Computer Uptime** - Shows how long the monitored computer has been working. By comparing the computer's uptime with the service's uptime (see above) you can always see whether or not DeviceLock Service was stopped during the current computer's session.
- **Service Version** - The version of the DeviceLock Service. Last five digits indicate the build number.

## Monitoring Algorithm

The algorithm used in the monitoring process is simple but effective:

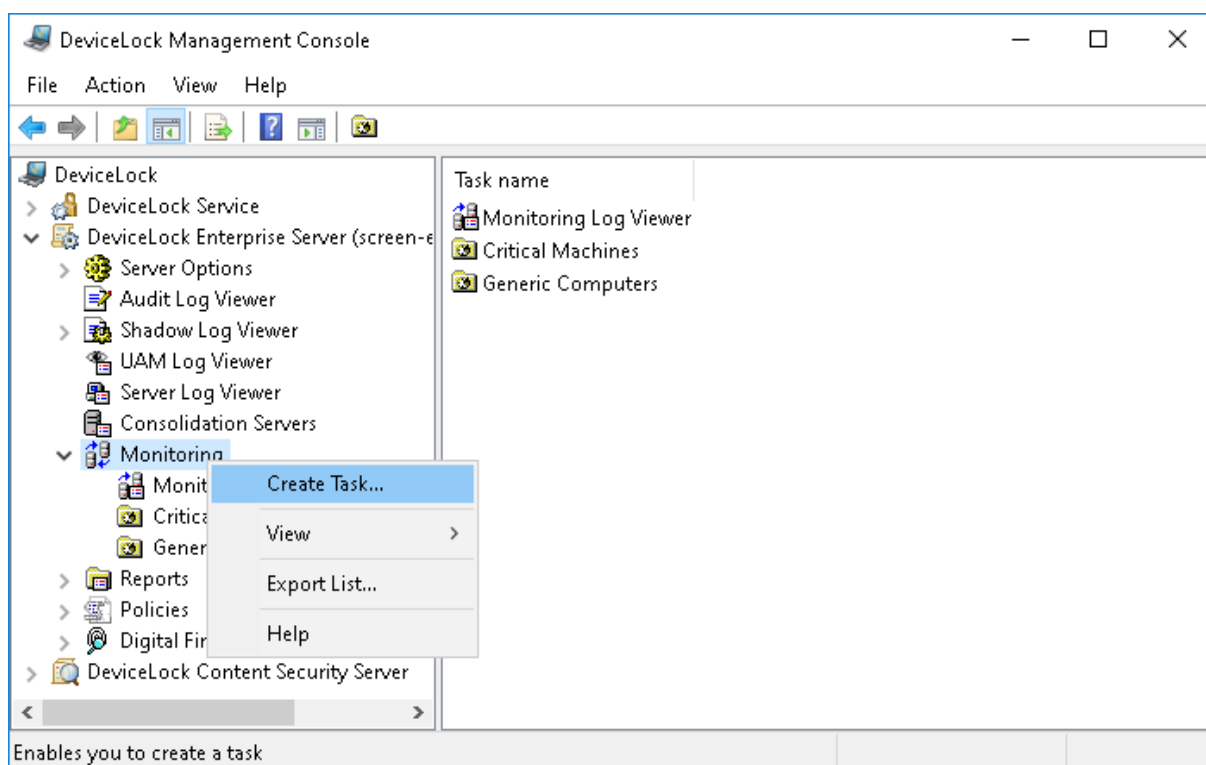
1. First of all DeviceLock Enterprise Server tries to scan the monitored computer to determine whether or not it is working. If the scan succeeds then the computer receives the **available** status and computer monitoring continues. Otherwise, it receives the **unavailable** status and computer monitoring stops (the record is written to the monitoring log).
2. Then DeviceLock Enterprise Server tries to connect to DeviceLock Service. If the connection succeeds then DeviceLock Service receives the **available** status and computer monitoring continues. Otherwise, it receives the **unavailable** status and computer monitoring stops (the record is written to the monitoring log).
3. If this task should verify DeviceLock Service policy integrity then computer monitoring continues. Otherwise, computer monitoring stops (nothing logged).
4. DeviceLock Enterprise Server downloads the policy from DeviceLock Service and compares it with the master policy assigned to this task. If no difference is found computer monitoring stops (nothing logged). If there is a difference between the two policies then computer monitoring continues (the record is written to the monitoring log).

5. If this task should restore the broken policy, then DeviceLock Enterprise Server writes the master policy to DeviceLock Service and computer monitoring stops (the record is written to the monitoring log). Otherwise, computer monitoring just stops (nothing logged).

If some error occurs at any step described above, then the record about that will be written to the monitoring log. If this error is not critical, computer monitoring may continue. If it is a critical error then computer monitoring stops. Also, some very critical errors (such as “no memory”) can halt execution of the whole task.

## Create/Edit Task

Each task contains its own set of computers, actions and configuration parameters.



To create a new task, use **Create Task** from the shortcut menu of the **Monitoring** item. To edit an existing task, select this task in the console tree and use **Edit Task** from the shortcut menu. If you wish to delete the task permanently, select this task in the console tree and use **Delete Task** from the shortcut menu.

The following dialog box is used to create or edit a monitoring task:

**Create Task**

Name:

☒ Active

Computers:

Network discovery methods:

☐ Ping sweep

☒ NetBIOS queries

☐ TCP djscovery (ports):

Service connection settings:

☒ Dynamic ports

☐ Fixed TCP port:

☒ Verify Service Settings:

Service Settings file:

☐ Restore Service Settings

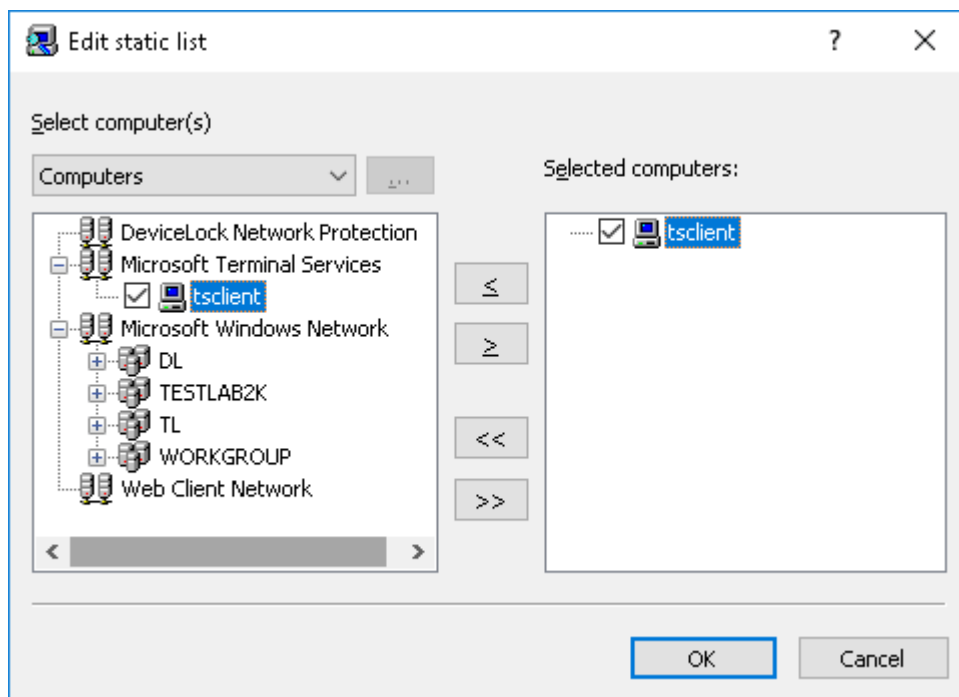
Scanning interval:    sec

Number of scanning threads:

☐ Install/Update DeviceLock Service automatically

☐ Remove DeviceLock Service automatically


- **Name** - The name of the task identifies this task in the tasks list and in the monitoring log (see [Monitoring Log Viewer](#)).
- **Active** - If selected, allows DeviceLock Enterprise Server to execute this task. Clear this check box if you wish to disable the task but do not want to delete it permanently.
- **Computers** - The type of the computers list used to define what computers will be monitored by this task.  
Click the **Edit** button to configure the list type selected in **Computers**.  
Two computer list types are supported:
  1. **Static list** - All of the computers are specified in the list by their names or IP addresses. Since this list is static, even if some computer no longer exists in the network, it will be monitored (and the error logged) until its record is deleted from the list manually.



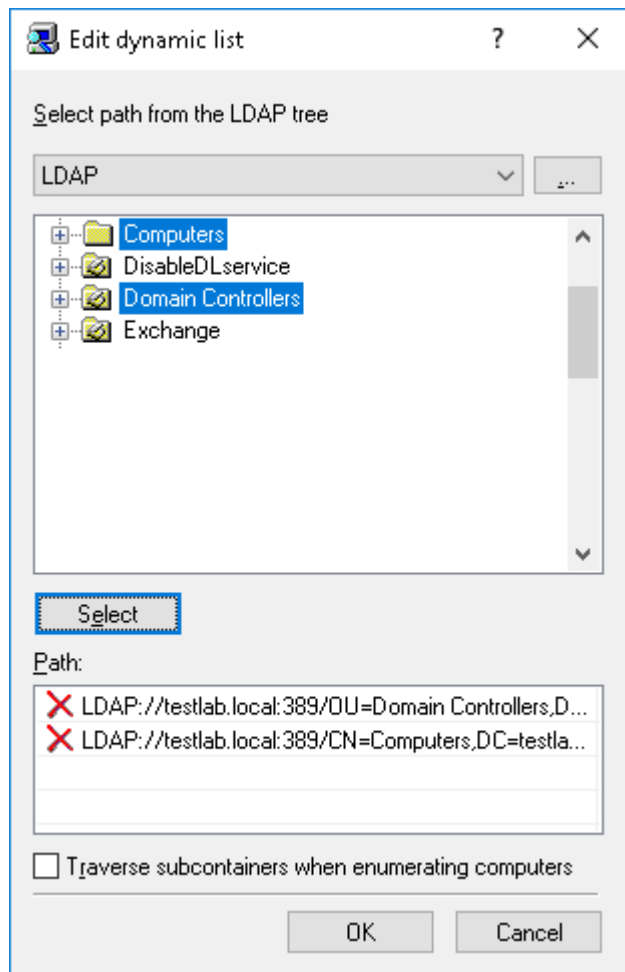
Computers that will be monitored should be specified in the right list. You have to select needed computers in the left list and then move them to the right list by clicking the button. If you need to exclude some computers from the monitoring process, select them in the right list and then click the button.

By using and buttons, you can add and remove all available computers at the same time (no need to select computers in the list).

There are several flexible ways to choose network computers from the left list:

- **Active Directory** - Browse and select computers from Active Directory organizational units (OUs).
  - **Computers** - Browse and select computers from the network tree.
  - **LDAP** - Browse and select computers from the tree of a LDAP (Lightweight Directory Access Protocol) compatible directory service.
  - **From File** - Load the list of computers from a text file and then select computers from that list. To open a file, click the  button. The file must contain each computer's name or IP address on a separate line.
  - **Manual** - Type computer names to select computers. Each computer's name or IP address must be typed on a separate line.
2. **Dynamic list** - Instead of computer names or IP addresses, the dynamic list contains a path to the container (for example, an organizational unit) in the directory service tree (such as Active Directory, Novell eDirectory, OpenLDAP and so on). Every time the task is executing, DeviceLock Enterprise Server retrieves all the computers that currently exist in this container. Hence, if some computer was removed from the directory tree or moved to another container it will not be monitored anymore. And vice versa, if there is some new computer that did not exist in the container at the time the task was created/modified, but was added to this container later, it will be retrieved and monitored at the time of executing the task. You can

select one or more containers.



The path to the selected containers is specified in the **Path** field. Select containers in the tree by clicking while holding down the Shift or Ctrl key. Then click the **Select** button. To deselect the container, click the red X in the **Path** field.

Select the **Traverse subcontainers when enumerating computers** check box to allow DeviceLock Enterprise Server to retrieve computers from all the nested containers located inside the selected container. Otherwise, if this check box is unselected all nested containers are ignored, and only computers located directly in the selected container are retrieved at the time of executing the task.

There are two modes to work with the directory service:

- **Active Directory** - Browse and select a container from the Active Directory tree. While the Active Directory tree can also be displayed by choosing the **LDAP** option (see below), the Active Directory mode results in greater efficiency between the directory service and DeviceLock Enterprise Server service and thus resource savings. If you need to supply alternative credentials to access Active Directory, click the **...** button to open the **Credentials** dialog box and specify the needed user account and its corresponding password.



---

**Note**

If no alternative credentials are specified when accessing Active Directory, DeviceLock Enterprise Server uses the credentials of the account under which its service started. For more information, see the [Log on as](#) parameter description.

---


Select the **Synchronization** check box to allow DeviceLock Enterprise Server to use the internal synchronization mechanisms provided by Active Directory. This will dramatically reduce the load on the domain controller and speed up the process of retrieving computers at the time of task execution.

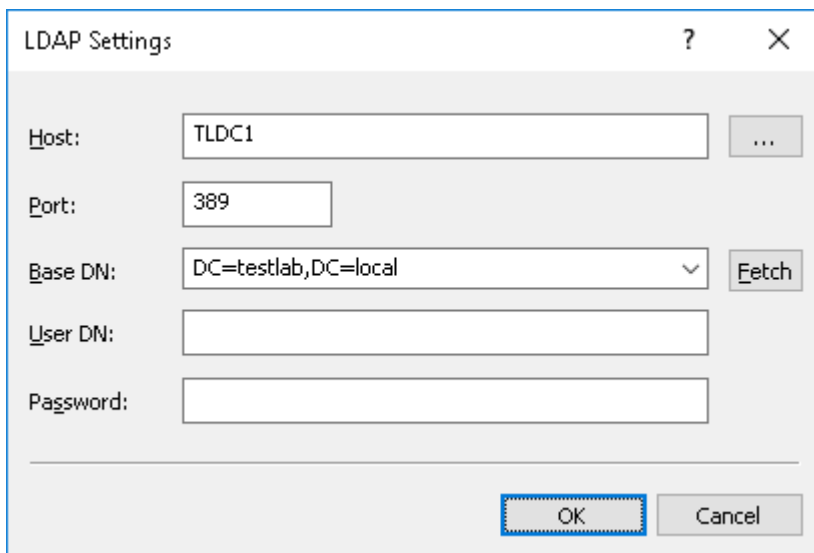
---

**Note**

Administrative access to Active Directory is required to use the synchronization function.

---

- **LDAP** - Browse and select a container from the tree of a LDAP (Lightweight Directory Access Protocol) compatible directory service.  
To configure a connection to the LDAP server, click the  button and open the **LDAP Settings** dialog box.



The image shows the 'LDAP Settings' dialog box. It has a title bar with a question mark and a close button. The dialog contains several input fields: 'Host' with the value 'TLDC1' and a button with three dots; 'Port' with the value '389'; 'Base DN' with a dropdown menu showing 'DC=testlab,DC=local' and a 'Fetch' button; 'User DN' and 'Password' are empty text boxes. At the bottom are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a blue dashed border.

- **Host** - The name or the IP address of the LDAP server to connect to.
- **Port** - The TCP port on which the LDAP server accepts connections. The default port is 389.
- **Base DN** - The starting point for you to browse the directory tree. You must use the LDAP string representation for distinguished names (for example, cn=qa,o=SMARTLINE,c=US). Leave the **Base DN** box blank to start browsing from the root.  
By clicking the **Fetch** button, you can get all the published naming contexts.
- **User DN** - The distinguished name (DN) of the directory user that allows connection to the directory. You must use the LDAP string representation for distinguished names (for example, cn=admin,o=SMARTLINE,c=US).

---

**Note**

If no user is specified when accessing the LDAP server, DeviceLock Enterprise Server uses the credentials of the account under which its service started. For more information, see the [Log on as](#) parameter description.

---

- **Password** - The user's password.
- **Network discovery methods** - Types of network scanning that will be used to determine the status (**available** or **unavailable**) of monitored computers.

Upon executing the task, DeviceLock Enterprise Server uses all selected discovery methods in their given order until the status **available** is returned for the target computer. If none of the selected methods returns the **available** status, then the target computer receives the **unavailable** status.

Three types of the network scan are supported:

- **Ping sweep** - DeviceLock Enterprise Server sends a regular ICMP ping to the target computer and then waits for its reply.
- **NetBIOS queries** - If the Client for Microsoft Networks is installed on the target computer, then this computer will answer the NetBIOS type query sent by DeviceLock Enterprise Server.
- **TCP discovery (ports)** - DeviceLock Enterprise Server checks for a particular open TCP port on the target computer. Using the comma (,) or semicolon (;) as a separator, you can specify several ports so they will be checked one by one in their given order.

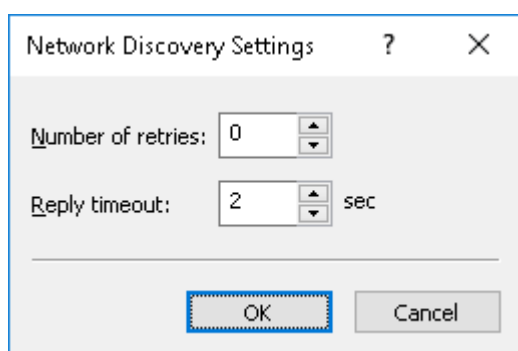
---

**Note**

A firewall running on a target computer can block the sending of some or all network packets so such a computer will be detected as unavailable even if it is up and running.

---

To define additional parameters for discovery methods, click the **Advanced Settings** button and open the **Network Discovery Settings** dialog box.



- **Number of retries** - The number of times that DeviceLock Enterprise Server will perform each type of scan when it returns the **unavailable** status. A value of zero (0) in this field means that no retries will be performed for that scan type after the first failed attempt.
- **Reply timeout** - The time in seconds DeviceLock Enterprise Server will wait for a response from the target computer for each type of scan. If DeviceLock Enterprise Server is running on a slow or busy network, you may need to increase this timeout.

- **Service connection settings** - These options define how DeviceLock Enterprise Server should connect to DeviceLock Services on the monitored computers to obtain service version, settings, etc. If the correct connection settings are not specified, DeviceLock Enterprise Server will not be able to connect to monitored services and their computers will not receive the **available** status. DeviceLock Service can be configured to use either a fixed port or dynamic ports during the installation process. For more information on this, see [Unattended Installation](#) and [Installation via DeviceLock Enterprise Manager](#).

There are two connection options:

- **Dynamic ports** - To instruct DeviceLock Enterprise Server to use dynamic ports for communication with DeviceLock Service, select this option.
- **Fixed TCP port** - If DeviceLock Service is configured to accept connections on a fixed port, then you should select this option and specify that port number.

---


#### Note

In order to successfully connect to monitored DeviceLock Services and obtain needed information from them, DeviceLock Enterprise Server must have at least Read-only access rights to these services. If this task also needs to write some settings to monitored DeviceLock Services, then DeviceLock Enterprise Server requires Full access rights to these services.

To connect to monitored DeviceLock Services, DeviceLock Enterprise Server uses the credentials of the account under which its service started. It can also use DeviceLock Certificate authentication, if a private key is specified. For more information, see the description of parameters [Log on as](#) and [Certificate Name](#).

---

- **Verify Service Settings** - Select this check box if you want the monitoring task to check DeviceLock Service settings by comparing them with particular master settings. When this check box is selected, the monitoring task on each monitored computer compares DeviceLock Service settings with those in the master policy. If any settings are detected that do not match the master policy, the status of the computer changes to "Settings are corrupted". In addition, a "Settings are corrupted" event is recorded in the monitoring log. The non-matching settings are listed in the event record, and can be inspected by using the View details command on the "Settings are corrupted" event in the [Monitoring Log Viewer](#). One more way to view the non-matching settings is by using the View details command on a monitored computer that has the status of "Settings are corrupted" (for details, see [Task and Its Monitored Computers](#)).
- **Service Settings file** - The path and name of the file that holds DeviceLock Service settings considered as the master policy. The button next to this field is used to select a file. The master policy is assigned to the task by loading a particular file with DeviceLock Service settings. This file can be created in the DeviceLock Management Console, DeviceLock Group Policy Manager and/or DeviceLock Service Settings Editor. When performing the check, the task gets the settings from the monitored computers and compares them with the settings file assigned as the master policy to that task. All non-configured settings (those that have the Not Configured state) in the master policy are disregarded during the check. This feature can be used to selectively verify the settings of interest, while allowing other settings to differ from the master policy.

To load a file, click the  button. Since the signature of the file is not validated at this step, a signed or non-signed file can be selected. The path and name of the selected file are displayed in the **Service Settings file** box. In the case of a signed file, the box displays the file's path and name embraced in parentheses.

When editing a task to which a master policy has already been assigned, the master policy settings can be exported to a file by clicking the **Save** button.

- **Restore Service Settings** - Select this check box if you want the monitoring task to replace the corrupted settings on the monitored computers with the settings from the master policy. When this check box is selected, the task not only checks DeviceLock Service settings but also restores them in case of their change or corruption.
- **Scanning interval** - The time in seconds that should pass after a task completes and before DeviceLock Enterprise Server will start executing the same task again.
- **Number of scanning threads** - The maximum number of threads that can be used by this task simultaneously. You can increase this number to parallelize the process of computer scanning. However, a larger number of threads requires more hardware resources (especially RAM and network bandwidth) for DeviceLock Enterprise Server.
- **Install/Update DeviceLock Service automatically** - Select this check box if you want to install DeviceLock Service to monitored computers.
- **Remove DeviceLock Service automatically** - Select this check box if you want to remove DeviceLock Service from monitored computers.

---

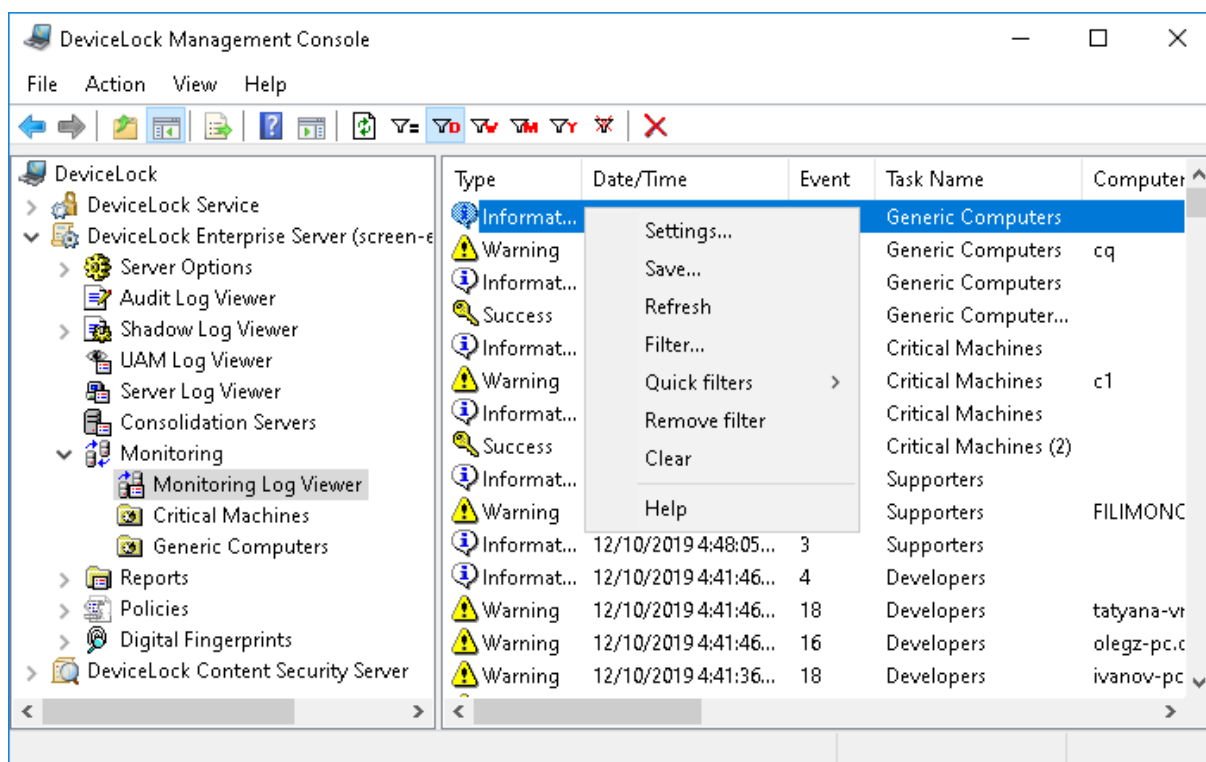
**Note**

If the DeviceLock Enterprise Server service is configured to run under the Local System account, you cannot install, update or remove DeviceLock Services on remote computers using a Monitoring task on DeviceLock Enterprise Server.

---

## Monitoring Log Viewer

This viewer allows you to retrieve the monitoring log. The monitoring log is used by tasks to write information about monitored computers and DeviceLock Services.



The columns of this viewer are defined as follows:


- **Type** - The event type can be one of the following:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Date/Time** - The date and time that the event occurred.
- **Event** - The ID number of the event.
- **Task Name** - The name of the monitoring task that caused the event. Can be blank if the event does not apply to a task.
- **Computer Name** - The name of the monitored computer that caused the event. Can be blank if the event does not apply to a monitored computer.
- **Information** - A description of the event that provides details on the actions performed and errors encountered.
- **Server** - The name of the computer running DeviceLock Enterprise Server that logged this event.
- **Record N** - Sequence number of the event record in the list.
- **Consolidation Server** - The name of the remote server from which this event was last received during log consolidation (see [Consolidating Logs](#)).
- **Consolidated Date/Time** - The date and time that this event was last received from the remote server during log consolidation (see [Consolidating Logs](#)).

## Managing the Monitoring Log






The log can be managed by using commands from the shortcut menu:

- In the DeviceLock Management Console tree, expand **DeviceLock Enterprise Server** > **Monitoring**, and then right-click **Monitoring Log Viewer**.  
- OR -
- In the DeviceLock Management Console tree, select **DeviceLock Enterprise Server** > **Monitoring** > **Monitoring Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides following commands:



- **Settings** - View or change the settings that limit the maximum number of records the log may contain (see [Monitoring Log Settings](#)).
- **Save** - Save the log to the file you specify.
- **Refresh**  - Update the list of event records with the latest information.
- **View details** - For a “Settings are corrupted” event, review the DeviceLock Service settings on the monitored computer that do not match the master policy defined in the monitoring task (see the [Verify Service Settings](#) parameter description).

The **View details** command opens a dialog box that lists the non-matching settings, with each setting followed by a description of the mismatch, such as:

- **non-existent** - The setting is specified in the master policy, but is missing from the monitored computer.
  - **changed** - The setting is specified differently in the master policy and on the monitored computer.
  - **excessive** - The setting is marked as deleted in the master policy, but is specified on the monitored computer.
- **Filter**  - Display only the records that match the conditions specified (see [Monitoring Log Filter](#)).
  - **Quick filters** - Choose from the following options to display only records for a certain period of time:
    - Current day 
    - Current week 
    - Current month 
    - Current year 

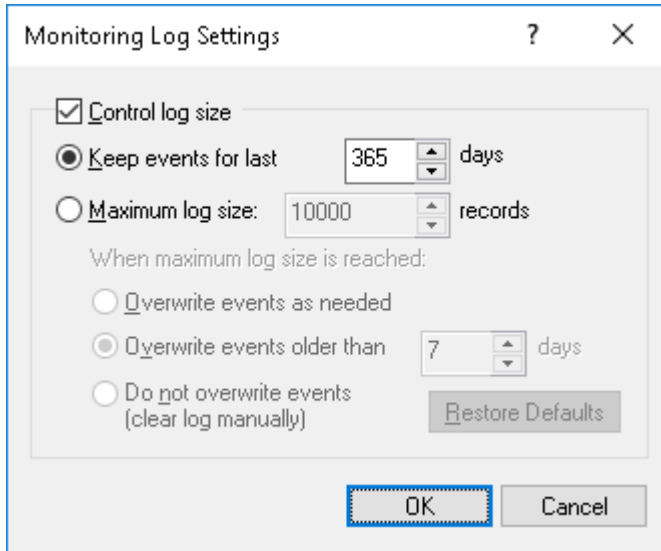
To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Clear**  - Delete all records that currently exist in the log.

## Monitoring Log Settings

To control the log size and server actions when the log is overflowing, select the **Settings** command from the shortcut menu of this log viewer in the console tree. Then, view or change the settings in the dialog box that appears.



The log settings are similar to those of the Audit log, see [Audit Log Settings \(Server\)](#).

---

### Note

The server removes old records either by the date indicated in the **Date/Time** column (for records logged by the local server) or by the date indicated in the **Consolidated Date/Time** column (for records received from other servers using [consolidation](#)).

---

## Monitoring Log Filter

By using a filter, the [Monitoring Log Viewer](#) can be configured to display only the records that meet particular conditions. To view or change these conditions, select **Filter** from the shortcut menu or click the corresponding button on the toolbar, and then use the dialog box that appears.

The monitoring log filter is configured in the same way as the audit log filter described in [Audit Log Filter \(Server\)](#).

Two types of filter are available:

- **Include** - Display only the event records that match the condition specified. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab and specify conditions on that tab.
- **Exclude** - Do not display the event records that match the conditions specified. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab and specify conditions on that tab.

The filter can be temporarily disabled by clearing the **Enable filter** check box.

---

#### Note

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

When the filter is enabled, its conditions are defined by entering values in the following fields:



- **Event types** - Select check boxes to filter event records by type:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- String fields intended to include or exclude event records depending upon whether event data matches the filter string specified. For example, to filter records by the name of the task that caused the event, specify a filter string in the **Task name** field. To filter records with certain event IDs, enter ID numbers separated by a semicolon in the **Event ID** field.  
The following string fields are available:
  - **Computer name** - The name of the monitored computer that caused the event.
  - **Task name** - The name of the monitoring task that caused the event.
  - **Information** - A description of the event that provides details on the actions performed and errors encountered.
  - **Server** - The name of the computer running DeviceLock Enterprise Server that logged the event.
  - **Event ID** - The ID number of the event.

---

#### Note

To assist with configuring a filter, string fields store previous entries and suggest matches for what you are typing. Previous entries are also available on the drop-down list of options for the setting field.

---

- **From, To** - The time range settings to filter events by time they were logged by the server.
- **Consolidation** - The fields to filter by log consolidation-related data (see [Consolidating Logs](#)):
  - **Server** - The name of the remote server from which the event was last received during log consolidation. This field is case-insensitive, and allows the use of wildcards (\* and ?). To enter multiple values, separate them with a semicolon (;).
  - **From, To** - The time range settings to filter events by time they were last received from the remote server during log consolidation.

For each time range, the following settings are available:

- **From** - The beginning of the time range. Possible values:
  - **First Record** - Filter starting with the earliest date and time in the respective log field.
  - **Records On** - Filter starting with a particular date and time.
- **To** - The end of the time range. Possible values:
  - **Last Record** - Filter ending with the latest date and time in the respective log field.
  - **Records On** - Filter ending with a particular date and time.

---

**Note**

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

# DeviceLock Enterprise Server Policies

## Overview

This functionality of DeviceLock Enterprise Server allows you to automatically distribute DeviceLock security policies to client computers on the network. If such policies are configured, client computers will always initiate connections to DeviceLock Enterprise Server and request a policy from it, thus eliminating the need to check whether the client computers are running or not. This greatly simplifies and optimizes security policy management, especially in a non-Active Directory environment or as an alternative to Group Policy.

DeviceLock Enterprise Server also provides the Policy Log to help you troubleshoot issues with execution of DeviceLock policies. This log records events generated during the runtime of a policy.

Configuration of a policy is based on a certain file that determines DeviceLock Service settings (.dls file). You can create a .dls file by using the DeviceLock Management Console when connected to a single endpoint. A better option is to use the DeviceLock Service Settings Editor console for that purpose.

## How Policies Are Processed and Applied

You can use policies to define configurations for lists of endpoint client computers. Policies are a collection of policy objects. Each policy object contains four main elements: a name, a list of computers to which this policy object is applied, configuration settings specified in a DeviceLock Service settings file (.dls), and a priority used to resolve conflicting policy settings among different policy objects. If there are policy setting conflicts between two policy objects, the policy object with a higher assigned priority wins, and its settings are applied. The priority value can range from 0 to 100, with 0 being the lowest priority and 100 being the highest priority. For a client computer that is assigned two or more policies with the same priority, the first policy received from the server takes priority and is applied first.

You can create your own policy objects or use the Default Policy object included with DeviceLock Enterprise Server. The Default Policy is automatically applied to all client computers regardless of any other applied policy objects. You cannot delete this policy, but you can block inheritance of it. Blocking inheritance of the Default Policy prevents the application of the policy. You can also partially modify it to suit your needs. In the Default Policy object, you can, for example, assign a policy by loading a DeviceLock Service settings file (.dls) or change a static list of client computers to which the policy is applied. You cannot change the name nor the priority of the Default Policy object. The Default Policy has the lowest priority. When multiple policy objects are applied to a client computer, the resultant policy that contains the sum of all settings from the policy objects is applied. If there are conflicting policy settings among these policy objects, the non-default policy takes priority over the Default Policy.

Once you have defined policy settings in policy objects, they are ready to be enforced. A client/server interaction works as follows:

- A client computer locates a specific server that was chosen for connection and sends a policy request to the server to initiate a connection. The policy request contains a checksum of the client's current policy settings.

A policy request from a client is sent either every hour or when any of the following events occurs:

- A user boots or reboots the computer running DeviceLock Service.
- A user logs on.
- A user right-clicks the DeviceLock Tray Notification Utility icon in the notification area of the taskbar, and then clicks **Refresh Current State**.

The DeviceLock Tray Notification Utility icon is displayed in the notification area when [Always show tray icon](#) is enabled in [Service Options](#).

- DeviceLock Service switches from offline mode to online mode.

---

#### Note

Policies can be received only from the servers assigned to the Everyone account. The servers assigned to specific user accounts are not used for policy distribution, but only for audit log and shadow file collection.

---

- The server determines which policy objects are applied to the client computer, creates a resultant policy for it by merging settings from the policy objects, and then compares the checksums of the current policy and the resultant policy. If the policy checksum comparison finds these policies are different, the server returns the resultant policy to the client. If the policies are identical, the policy transfer does not occur.

---

#### Note

- If there is a list of DeviceLock Enterprise Servers that DeviceLock Service can connect to, and the initial server chosen for connection fails to send the requested policy to the client, the client then selects the next server in the list.
  - If the client has the DeviceLock Certificate (the public key), the server chosen for connection must also have the corresponding certificate (the private key). Otherwise, the policy transfer fails.
- 

## Policy Application Scenarios: Required Configuration Steps

There are two main scenarios for applying DeviceLock Enterprise Server policies to client computers. The scenarios also describe configuration steps needed for successful policy enforcement.

### ***Policy Application Scenario 1***

In this scenario, the pre-configured agent (DeviceLock Service) running on a client computer connects to a specified DeviceLock Enterprise Server and receives the appropriate policy. Before you start to use this scenario, make sure that you have set the following service options:

- **DeviceLock Enterprise Server(s)** - Specifies a list of servers that DeviceLock Service can connect to.
- **Policy Source(s)** - Specifies the policy application mode for DeviceLock Service.

The following procedures provide instructions for setting these options.

#### **To configure DeviceLock Enterprise Server(s)**

1. If you use DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If you use DeviceLock Service Settings Editor, do the following:
    - a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If you use DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Select **Service Options**.  
*When you select Service Options in the console tree, they are displayed in the details pane.*
3. In the details pane, do one of the following:
  - Right-click **DeviceLock Enterprise Server(s)**, and then click **Properties**.  
- OR -
  - Double-click **DeviceLock Enterprise Server(s)**.  
*The DeviceLock Enterprise Server(s) dialog box appears.*
4. In the **DeviceLock Enterprise Server(s)** list, double-click the **Servers** field next to the **Everyone** account, and then type the name or IP address of the computer running DeviceLock Enterprise Server. You can enter multiple names or IP addresses by separating them with a semicolon (;).  
*Policies can be received only from the servers assigned to the Everyone account.*

---

#### **Note**

Make sure that DeviceLock Enterprise Server is properly installed and accessible to DeviceLock Service.

---

To make changes to the **Servers** field, double-click that field (another option is to click **Edit** or press F2).

5. Click **OK**.

#### **To configure Policy Source(s)**

1. If you use DeviceLock Management Console, do the following:
  - a. Open DeviceLock Management Console and connect it to the computer running DeviceLock Service.
  - b. In the console tree, expand **DeviceLock Service**.  
If you use DeviceLock Service Settings Editor, do the following:

- a. Open DeviceLock Service Settings Editor.
  - c. In the console tree, expand **DeviceLock Service**.  
If you use DeviceLock Group Policy Manager, do the following:
    - a. Open Group Policy Object Editor.
  - d. In the console tree, expand **Computer Configuration**, and then expand **DeviceLock**.
2. Select **Service Options**.  
*When you select Service Options in the console tree, they are displayed in the details pane.*
3. In the details pane, do one of the following:
  - Right-click **Policy Source(s)**, and then click **Properties**.  
- OR -
  - Double-click **Policy Source(s)**.*The Policy Source(s) dialog box appears.*
4. In the **Policy Source(s)** dialog box, click any of the following options:
  - **Local & GPO** - Indicates that a client computer applies either Group Policy or local computer policy, while the DeviceLock Enterprise Server policy is ignored.
  - **Local & Enterprise Server** - Indicates that a client computer applies either the DeviceLock Enterprise Server policy or local computer policy, while Group Policy is ignored.
5. Click **OK**.

When these settings are set, you can configure DeviceLock Enterprise Server to send the appropriate policy to agents. For more information, see the [Managing DeviceLock Policies](#) section.

### **Policy Application Scenario 2**

In this scenario, the previously installed agent has been updated to the latest version (with DeviceLock Enterprise Server policies) and can now receive the DeviceLock Enterprise Server policy in the server-push mode. This scenario requires that the following condition is met:

- The **Policy Source(s)** service parameter is either not specified or is set to **Local & Enterprise Server**.

For more information on the **Policy Source(s)** parameter, see the procedure [To configure Policy Source\(s\)](#) earlier in this section.

For more information on the server-push procedure, see the [Immediately Applying Policies to Client Computers](#) section later in this document.

## Managing DeviceLock Policies

The management of DeviceLock policies involves the following:

- [Using the Policies Node](#)
- [Managing Policy Objects](#)
- [Managing Computers Assigned to Policy Objects](#)
- [Using the Policy Log Viewer](#)

## Using the Policies Node

DeviceLock Enterprise Server allows you to automatically distribute DeviceLock security policies to client computers on the network. If such policies are configured, client computers will always initiate connections to DeviceLock Enterprise Server and request a policy from it, thus eliminating the need to check whether the client computers are running or not. This greatly simplifies and optimizes security policy management, especially in a non-Active Directory environment or as an alternative to Group Policy.

DeviceLock Enterprise Server policies are a collection of policy objects. Each policy object contains four main elements: a name, a list of computers assigned to that policy object, configuration settings specified in a DeviceLock Service settings file (.dls), and a priority used to resolve conflicting policy settings among different policy objects. All policy objects that currently exist on the server are listed in the console tree under **DeviceLock Enterprise Server > Policies**.

When you select the **Policies** node in the console tree, the details pane lists the policy objects that currently exist on the server. The list in the details pane displays the following information on each policy object:

- **Policy Object Name** - The name of the policy object
- **Last Update Time** - The date and time that the policy object was last changed.
- **Settings File** - The name of the DeviceLock Service settings (.dls) file that determines the DeviceLock Service settings for the policy object.
- **Author** - The account of the user who created this policy object.
- **Priority** - The priority value of the policy object. Higher value indicates higher priority.
- **Policy Object ID** - A unique numeric identifier of the policy object.

The shortcut menu on the **Policies** node includes the following command:

- **Create Policy Object** - Creates a new policy object. You can specify the desired settings for the new policy object in the dialog box that appears when you select this command. For details, see [Creating a Custom Policy Object](#).

The shortcut menu on a policy object in the details pane includes the following commands:

- **Edit Policy Object** - Opens a dialog box where you can view or change the settings of the selected policy object.
- **Edit Computers List** - Opens a dialog box where you can view or change the list of computers assigned to this policy object.
- **Load Policy** - Allows you to load or replace the DeviceLock Service settings (.dls) file in the policy object. You can open the desired settings file in the dialog box that appears when you select this command.

This file saves DeviceLock Service settings. You can create a settings file by using the DeviceLock Management Console connected to a computer running DeviceLock Service. A better option would be to use the DeviceLock Service Settings Editor console for that purpose.

- **Save Policy** - Allows you to save the policy settings to a DeviceLock Service settings (.dls) file. You can specify a file in the dialog box that appears when you select this command. Saving policy settings to a file might be helpful when you want to load them to another policy object. In this case, you can successively use the **Save Policy** and **Load Policy** commands.
- **Delete Policy Object** - Deletes the selected policy object.
- **Deploy Now** - Sends the policy from the selected policy object immediately to all computers assigned to that policy object. In case of multiple policy objects assigned to those computers, the command will send them the resultant policy from all objects.
- **Refresh** - Updates the list in the details pane with the most recent information. Since the console does not automatically update information displayed in the details pane, you need to update the list by using the **Refresh** command.

## Policy Object

DeviceLock Enterprise Server policies are a collection of policy objects. Each policy object contains four main elements: a name, a list of computers assigned to that policy object, configuration settings specified in a DeviceLock Service settings file (.dls), and a priority used to resolve conflicting policy settings among different policy objects.

The console displays policy objects in the console tree under **DeviceLock Enterprise Server > Policies**.

When you select a policy object in the console tree, the details pane lists the computers assigned to that policy object. The list in the details pane displays the following information on each computer:

- **Computer Name** - The name that identifies the computer.
- **Status** - The current status of the computer. The possible statuses and their associated icons are as follows:
  - Icon: Gray computer, status: **(empty)**. A temporary status that appears immediately after creation of the policy object. This status changes after the first attempt of DeviceLock Enterprise Server to establish a connection to DeviceLock Service and enforce a policy on it.
  - Icon: Green computer, status: **Computer is available**. This status indicates that the computer is working and DeviceLock Service is running on it.
  - Icon: Green computer with exclamation point, status: **Group Policy is in use**. This status indicates that Group Policy is applied and DeviceLock Enterprise Server is unable to push a policy.
  - Icon: Green computer with exclamation point, status: **Local Policy is in use**. This status indicates that local computer policy is applied because DeviceLock Service has the **Use Group/Server Policy** setting disabled.
  - Icon: Green computer with exclamation point, status: **Acronis Cyber Protect Policy is in use**. This status indicates that DeviceLock Service uses the policy received from the Acronis cyber protection system and ignores the policies from any other source.
  - Icon: Red computer, status: **Computer is unavailable**. This status indicates that DeviceLock Enterprise Server is unable to connect to DeviceLock Service on the client computer.



- Icon: Red computer with exclamation point, status: **Unresolved computer address**. This status indicates that DeviceLock Enterprise Server is unable to resolve the name/address of the client computer.
  - Icon: Green computer with exclamation point, status: **Unsupported service version**. This status indicates that DeviceLock Enterprise Server is trying to enforce policies on DeviceLock Service version 8.1 or earlier client versions. Policy enforcement is supported only for version 8.2 or later versions. This status can also indicate that the service version is newer than the server version.
  - Icon: Green computer with exclamation point, status: **Access is denied**. This status indicates that DeviceLock Enterprise Server is unable to connect to DeviceLock Service due to lack of privileges. This happens when the account under which the DeviceLock Enterprise Server service starts has no rights to connect to DeviceLock Service. This status can also indicate that the certificate (the public key) installed on DeviceLock Service and the certificate (the private key) installed on DeviceLock Enterprise Server do not match.
  - Icon: Green computer with exclamation point, status: **No License**. This status indicates that DeviceLock Enterprise Server is unable to enforce policies on the client computer running DeviceLock Service due to an insufficient number of licenses. DeviceLock Enterprise Server handles as many DeviceLock Services as there are licenses loaded into DeviceLock Enterprise Server.
  - Icon: Red computer with exclamation point, status: **Error**. This status indicates all other unspecified errors that are not described above and that can occur during policy application on client computers.
- **Last Deployment Time** - The date and time when the policy was last applied in the following format: dd.mm.yyyy hh:mm:ss, for example, 20.12.2016 13:55:28.
  - **Last Connect Time** - The date and time when connection was last established in the following format: dd.mm.yyyy hh:mm:ss, for example, 20.12.2016 13:55:28.
  - **Assigned Policy Objects** - The names of all policy objects assigned to this computer. The names are separated by commas and listed in priority order, from highest to lowest priority.
  - **Applied Policy Objects** - The names of the policy objects that have already been applied to the computer. The names are separated by commas and listed in priority order, from highest to lowest priority.
  - **Service Version** - The version number and build number of DeviceLock Service.

The shortcut menu on a policy object in the console tree provides the same commands as the policy object's menu in the details pane. For description of the commands, see [Using the Policies Node](#).

The shortcut menu on a computer in the details pane provides the following commands:

- **Connect to DeviceLock Service** - Connects the DeviceLock Management Console to DeviceLock Service running on that computer.
- **Edit Policy Object** - Opens a dialog box where you can view or change the settings of the policy object selected in the console tree.

- **Edit Computers List** - Opens a dialog box where you can view or change the list of computers assigned to the selected policy object.
- **Assign to Policy Object** - Allows you to specify the policy objects for the given computer. You can select or clear check boxes in the list of policy objects displayed by this command, assigning or removing the computer from the policy objects depending upon your selection.  
If you select multiple computers, the **Assign to Policy Object(s)** command assigns all the selected computers to the selected policy objects. The complementary command **Remove from Policy Object(s)** removes all the selected computers from the selected policy objects.
- **Exclude from All Policy Objects** - Removes the computer from all policy objects.  
As a result, the computer will receive only the Default Policy object if the DeviceLock Service on that computer is configured to use DeviceLock Enterprise Server policies.
- **Load Policy** - Allows you to load or replace the DeviceLock Service settings (.dls) file in the policy object. You can open the desired settings file in the dialog box that appears when you select this command.  
This file stores DeviceLock Service settings. You can create a settings file by using the DeviceLock Management Console connected to a computer running DeviceLock Service. A better option would be to use the DeviceLock Service Settings Editor console for that purpose.
- **Save Policy** - Allows you to save the policy settings to a DeviceLock Service settings (.dls) file. You can specify a file in the dialog box that appears when you select this command.  
Saving policy settings to a file might be helpful when you want to load them to another policy object. In this case, you can successively use the Save Policy and Load Policy commands.
- **Delete Policy Object** - Deletes the policy object selected in the console tree.
- **Deploy Now** - Sends the policy from the policy object selected in the console tree immediately to all computers assigned to that policy object. In case of multiple policy objects assigned to those computers, the command will send them the resultant policy from all objects.
- **Refresh** - Updates the list of computers with the latest information.  
Since the console does not automatically update information displayed in the list of computers, you need to update the list by using the **Refresh** command.

## Default Policy

The **Default Policy** object is a built-in policy object that DeviceLock Enterprise Server may automatically apply to all client computers regardless of any other applied policy objects. For further details, see [How Policies Are Processed and Applied](#).

You can partially modify the **Default Policy** object to suit your needs. For example, you can load a DeviceLock Service settings file (.dls) or set up a static list of computers for that object.

The console displays the **Default Policy** object in the console tree under **DeviceLock Enterprise Server > Policies**.

The shortcut menu on the **Default Policy** object provides the same commands as the menu on a regular policy object. For description of the commands, see [Policy Object](#).

When you select the **Default Policy** object in the console tree, the details pane lists the computers assigned to that object. For description of the computer list, see [Policy Object](#).

The shortcut menu on a computer in the details pane provides the same commands as in the case of a regular policy object. For description of the commands, see [Policy Object](#).

## Managing Policy Objects

DeviceLock policies are managed through, and enforced by, policy objects. You can create your own (custom) policy objects or use the Default Policy object included with DeviceLock Enterprise Server.

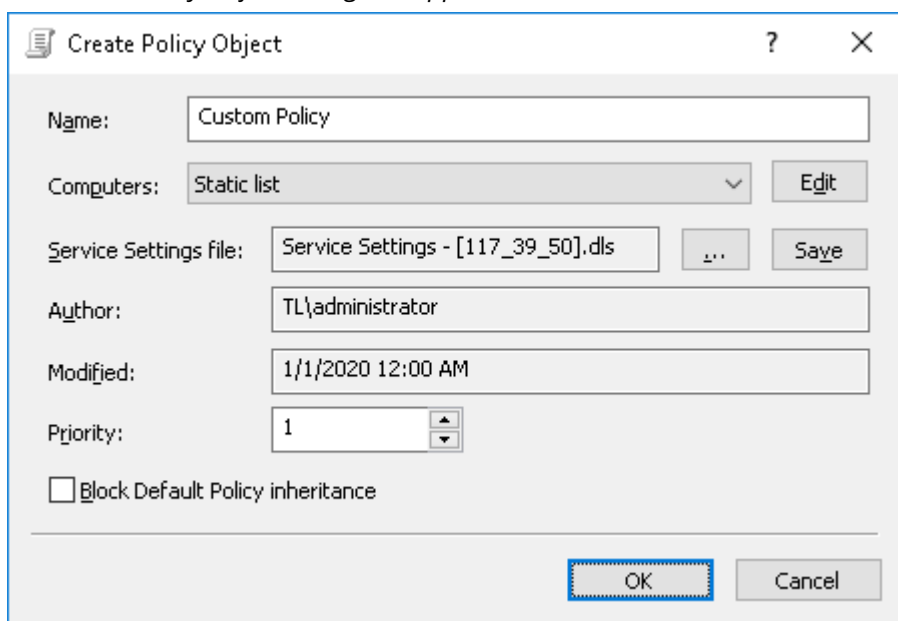
Managing policy objects involves the following tasks:

- [Creating a Custom Policy Object](#)
- [Editing a Policy Object](#)
- [Deleting a Custom Policy Object](#)
- [Restoring the Default Settings for the Default Policy Object](#)

### Creating a Custom Policy Object

#### *To create a custom policy object*

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, right-click **Policies**, and then click **Create Policy Object**.  
*The Create Policy Object dialog box appears.*



4. In the **Create Policy Object** dialog box, do the following:
  - **Name** - Specify the name of the policy object.
  - **Computers** - Assign the computers to the policy object. To do so, select either the **Static list** or **Dynamic list** option, and then configure the computer list as appropriate to your requirements.

- **Static list** - This option lets you specify a static list of computers assigned to the policy object. If you choose this option:
  - a. Click **Edit** to open the **Edit static list** dialog box.
  - b. In the **Edit static list** dialog box, select computers using one of the following options: **Active Directory, Computers, LDAP, From File, Manual**.
    - **Active Directory** lets you browse Active Directory OUs and select computers.
    - **Computers** lets you browse the network tree and select computers.
    - **LDAP** lets you browse the LDAP tree and select computers from the directory.
    - **From File** lets you import a list of computers from a text file and then select computers. To open such a file, click the **...** button. A text file must contain each computer's name or IP address on a separate line and can be either Unicode or non-Unicode.
    - **Manual** lets you type computer names manually to select computers. Each computer's name or IP address must be typed on a separate line.

*All selected computers are displayed in the right pane of the dialog box.*

*To remove single computers from the list of selected computers, use the left single-arrow button **<**. To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button **>>** or left double-arrow button **<<**.*
- **Dynamic list** - This option lets you specify a dynamic list of computers that will update automatically as new computers are added or removed from a certain container in the directory. If you choose this option:
  - a. Click **Edit** to open the **Edit dynamic list** dialog box.
  - b. In the **Edit dynamic list** dialog box, browse the AD or LDAP tree to find the required container, and then click **Select**. You can select one or more containers. To include computers located in lower-level containers within the one you selected, select the **Traverse subcontainers when enumerating computers** check box. To perform Active Directory synchronization, select the **Synchronization** check box. Click the **...** button to open either the **Credentials** or **LDAP Settings** dialog box. The **Credentials** dialog box opens if you selected the **Active Directory** option, while the **LDAP Settings** dialog box opens if you selected the **LDAP** option. Use the **Credentials** dialog box to specify the user account with administrative access rights to AD. Use the **LDAP Settings** dialog box to configure a connection to the LDAP server.
- **Service Settings file** - Assign a policy to the policy object by loading a DeviceLock Service settings file (.dls). To do so, click the **...** button to load the settings (.dls) file with the preferred DeviceLock Service settings. All unconfigured settings are ignored when multiple policies are merged. When being applied to DeviceLock Service, all unconfigured settings reset the corresponding parameters to their default values. To export the currently assigned policy to an external file, click **Save**.
- **Priority** - Specify a priority value ranging from 0 through 100, where 0 is the lowest priority and 100 is the highest priority. The policy's priority is used to resolve conflicting policy settings among different policy objects. If there are policy setting conflicts between two or more policy objects, the policy object with a higher priority wins, and its settings are applied.

- **Block Default Policy inheritance** - Disable the Default Policy for all computers assigned to the policy object. Select the **Block Default Policy inheritance** check box to disable the Default Policy. Clear the **Block Default Policy inheritance** check box to enable the Default Policy.

---

**Note**

If a client computer is assigned to two or more policy objects and at least one of these policy objects has the **Block Default Policy inheritance** option selected, the Default Policy will not be applied to the computer.

---

5. Click **OK** to close the **Create Policy Object** dialog box.

*The new policy object you created is added after the Default Policy object in the console tree.*

## Editing a Policy Object

You can edit an existing policy object as required to meet your needs.

### **To edit a policy object**

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Policies**, and do one of the following:
  - Right-click the policy object you want to edit, and then click **Edit Policy Object**.
  - OR -
  - Select the policy object you want to edit. In the details pane, right-click any computer assigned to the policy object, and then click **Edit Policy Object**.
4. In the **Edit Policy Object** dialog box that appears, edit the settings as appropriate.
5. Click **OK** to apply the changes.

## Deleting a Custom Policy Object

You can delete individual custom policy objects when they are no longer required. The Default Policy object cannot be deleted.

### **To delete a custom policy object**

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Policies**, and do one of the following:
  - Right-click the policy object you want to delete, and then click **Delete Policy Object**.
  - OR -
  - Select the policy object you want to delete. In the details pane, right-click any computer assigned to the policy object, and then click **Delete Policy Object**.

## Restoring the Default Settings for the Default Policy Object

You can reset the Default Policy object to its default settings by deleting the DeviceLock Service settings file (.dls) and the static list of client computers assigned to the policy.

### ***To restore the default settings for the Default Policy object***

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Policies**.
4. Under **Policies**, right-click **Default Policy**, and then click **Clear Policy Object**.

## Managing Computers Assigned to Policy Objects

Managing computers assigned to policy objects involves the following tasks:

- [Immediately Applying Policies to Client Computers](#)
- [Changing the Policy Object for a Client Computer](#)
- [Removing a Client Computer from All Policy Objects](#)
- [Refreshing a List of Assigned Computers and Policy Execution Information](#)

## Immediately Applying Policies to Client Computers

If a policy execution schedule does not meet your needs, you can force policies to be sent immediately from DeviceLock Enterprise Server to client computers. This server-push mode is also designed to be used in scenarios with agents that were not previously configured to use the DeviceLock Enterprise Server policy. For more information, see [Policy Application Scenario 2](#).

### ***To send policies to client computers immediately***

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Policies**, and do one of the following:
  - Right-click the desired policy object, and then click **Deploy Now**.  
*Doing so will force the policy from the selected policy object to be sent immediately to the client computers assigned to the policy object. If the computers from the selected policy object are also defined in other policy objects, a resultant policy from those policy objects will also be forced to be sent to the computers.*
  - OR -
  - Select the desired policy object. In the details pane, right-click any computer assigned to the policy object, and then click **Deploy Now**.  
*Doing so will force the policy from the selected policy object to be sent immediately to the selected client computer. If this computer is also defined in other policy objects, a resultant policy from those policy objects will also be forced to be sent to the computer.*

## Changing the Policy Object for a Client Computer

You can easily reassign the selected computer or a group of computers to the new policy object.

### ***To change the policy object for a computer***

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Policies**.
4. Under **Policies**, select the policy object with the desired computer.  
*When you select a policy object in the console tree, in the details pane you can view a list of all computers assigned to this policy object. You can also view policy execution information for each computer in the list.*
5. In the details pane, right-click the computer that you want to assign to a different policy object, point to **Assign to Policy Object**, and then click any desired policy object.  
*You can select multiple computers by holding down the SHIFT key or the CTRL key while clicking them.*

## Removing a Client Computer from All Policy Objects

If required, you can remove a specific client computer from all policy objects on DeviceLock Enterprise Server. Doing so will also remove the results of policy enforcement.

---

### **Note**

If the agent is still present and configured to use the DeviceLock Enterprise Server policy, it will send a policy request to the server and receive the Default Policy.

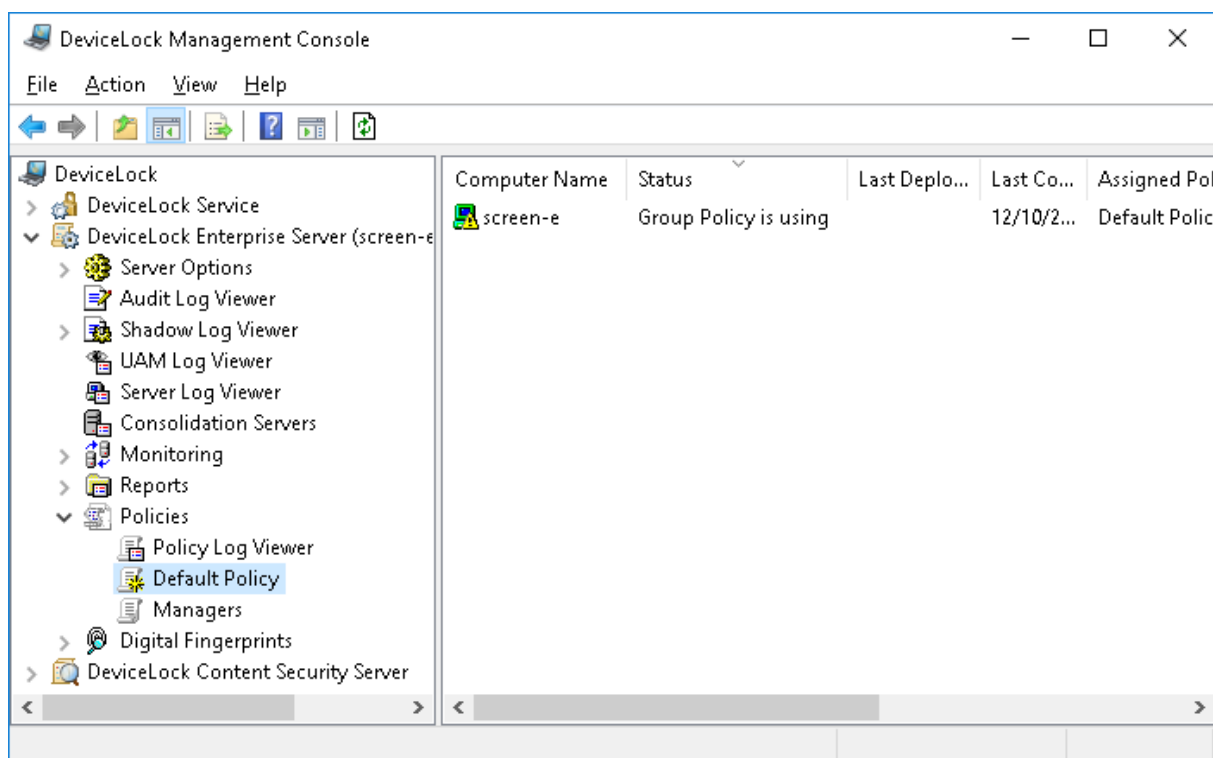
---

### ***To remove a client computer from all policy objects***

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, expand **Policies**.
4. Under **Policies**, select the policy object.  
*When you select a policy object in the console tree, in the details pane you can view a list of all computers assigned to this policy object. You can also view policy execution information for each computer in the list.*
5. In the details pane, right-click the computer you want to remove, and then click **Exclude from All Policy Objects**.

## Refreshing a List of Assigned Computers and Policy Execution Information

When you select any policy object in the console tree, the details pane allows you to view a list of all computers assigned to this policy object.



You can view policy execution information for each computer in the list. For description of the computer list, see [Policy Object](#).

Because the list of computers and policy execution information in the details pane are not updated automatically, you will need to perform a refresh operation.

#### ***To refresh a list of assigned computers and policy execution information***

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server** -> **Policies**.
3. Under **Policies**, right-click any policy object, and then click **Refresh**.

- OR -

Under **Policies**, select any policy object, and then do any of the following:

- Click **Refresh**  on the toolbar.

- OR -

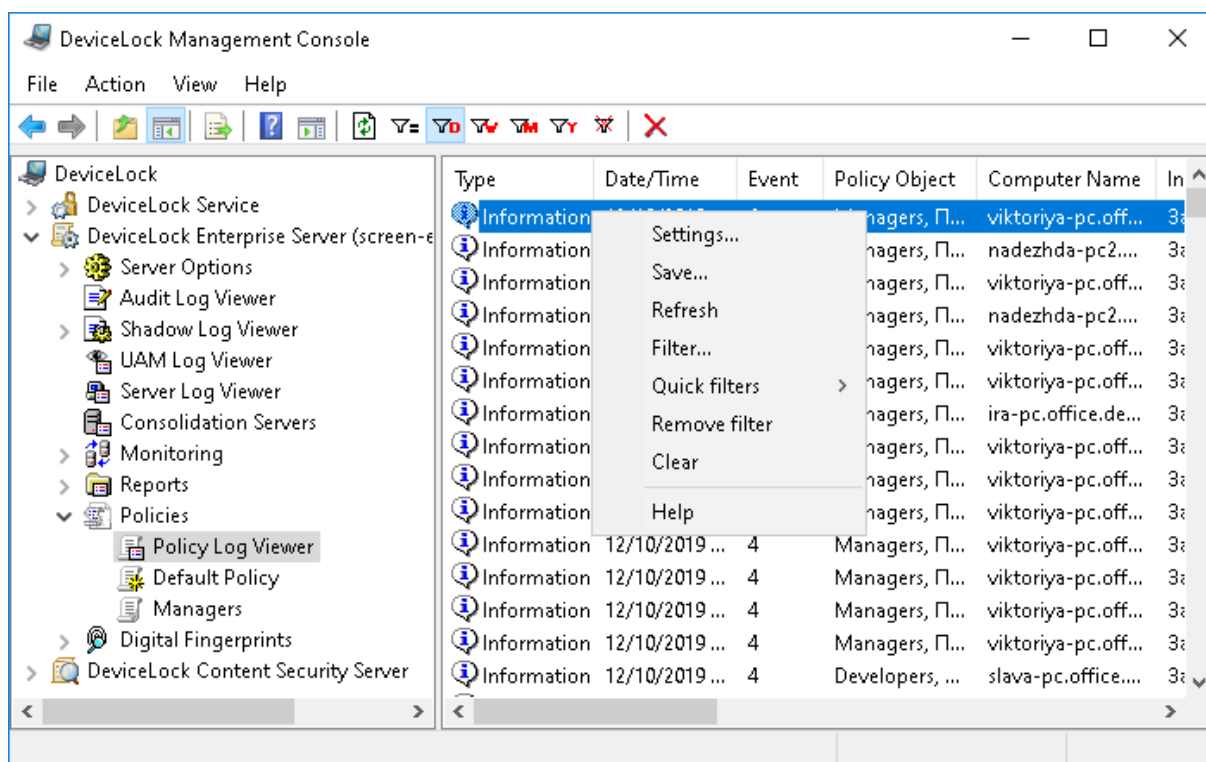
- Right-click in the details pane, and then click **Refresh**.

*When you select a policy object in the console tree, in the details pane you can view a list of all computers assigned to this policy object. You can also view policy execution information for each computer in the list.*

## Using the Policy Log Viewer

The Policy Log holds event records that can help you troubleshoot problems with management and execution of policies. To view the list of events, select **DeviceLock Enterprise Server** > **Policies** > **Policy Log Viewer** in the console tree.





The details pane in the console lists the events from the Policy Log, with the following information for each event:







- **Type** - The event type can be one of the following:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Date/Time** - The date and time that the event occurred.
- **Event** - The ID number of the event.
- **Policy Object** - The name of the policy object associated with the event.
- **Computer Name** - The name of the computer that caused this event.
- **Information** - A description of the event that provides details on the actions performed and errors encountered.
- **Server** - The name of the computer running DeviceLock Enterprise Server that logged this event.
- **Record N** - Sequence number of the event record in the list.
- **Consolidation Server** - The name of the remote server from which this event was last received during log consolidation (see [Consolidating Logs](#)).
- **Consolidated Date/Time** - The date and time that this event was last received from the remote server during log consolidation (see [Consolidating Logs](#)).

## Managing the Policy Log

The log can be managed by using commands from the shortcut menu:



- In the DeviceLock Management Console tree, expand **DeviceLock Enterprise Server > Policies**, and then right-click **Policy Log Viewer**.  
- OR -
- In the DeviceLock Management Console tree, select **DeviceLock Enterprise Server > Policies > Policy Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides following commands:

- **Settings** - View or change the settings that limit the maximum number of records the log may contain (see [Policy Log Settings](#)).
- **Save** - Save the log to the file you specify.
- **Refresh**  - Update the list of event records with the latest information.
- **Filter**  - Display only the records that match the conditions specified (see [Policy Log Filter](#)).
- **Quick filters** - Choose from the following options to display only records for a certain period of time:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Clear**  - Delete all records that currently exist in the log.  
This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.

## Policy Log Settings

To control the log size and server actions when the log is overflowing, use the **Settings** command from the shortcut menu of this log viewer in the console tree. This command displays a dialog box with the following settings:

- **Control log size** - Select this check box to allow the server to control the number of records in the log and delete outdated records. If this check box is cleared, the server uses all available database space to store the log.
- **Keep events for last <number> days** - When this option is selected, the log stores records no older than the number of days specified (365 days by default).
- **Maximum log size: <number> records** - When this option is selected, the log stores no more than the specified number of records. In this case, you must select the server action to be performed when the log reaches the maximum size:

- **Overwrite events as needed** - New event records continue to be stored when the maximum log size is reached. Each record of a new event replaces the oldest record in the log.
- **Overwrite events older than <number> days** - New event records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.
- **Do not overwrite events (clear log manually)** - New event records are not added when the maximum log size is reached. To enable the server to add new records, the log must be cleared by hand.

---

#### Note

The server removes old records either by the date indicated in the **Date/Time** column (for records logged by the local server) or by the date indicated in the **Consolidated Date/Time** column (for records received from other servers using [consolidation](#)).

---

#### Important

If the log has no space for new records and log settings do not allow the deletion of old records, then the server does not add any new records to the log.

---

To use default settings, click **Restore Defaults**. The default settings are as follows:

- Maximum log size: 10,000 records
- Overwrite events older than 7 days

## Policy Log Filter

Filter causes the list of events to display only the records that match the filter settings. To view or change these settings, click **Filter** on the shortcut menu. The filter settings are displayed in the **Filter** dialog box that appears:

Filter

☒ Include ☐ Exclude

Event types

☒ Success ☒ Warning

☒ Information ☒ Error

Computer name:

Policy Object:

Information:

Server:

Event ID:

From:

To:

Consolidation

Server:

From:

To:

☒ Enable filter

Clear Load Save

OK Cancel

In the **Filter** dialog box, you can use the following settings to configure a filter:

- **Include** - List only the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab.
- **Exclude** - Remove the events from the list that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab.

#### Note

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

- **Event types** - Select check boxes to filter event records by type:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.

- String fields intended to include or exclude event records depending upon whether event data matches the filter string specified. For example, to filter records by the name of the computer that caused the event, specify a filter string in the **Computer name** field. To filter records with certain event IDs, enter ID numbers separated by a semicolon in the **Event ID** field.

The following string fields are available:

- **Computer name** - The name of the computer that caused this event.
- **Policy Object** - The name of the policy object associated with the event.
- **Information** - A description of the event that provides details on the actions performed and errors encountered.
- **Server** - The name of the computer running DeviceLock Enterprise Server that logged the event.
- **Event ID** - The ID number of the event.

---

#### Note

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

- **From, To** - The time range settings to filter events by time they were logged by the server.
- **Consolidation** - The fields to filter by log consolidation-related data (see [Consolidating Logs](#)):
  - **Server** - The name of the remote server from which the event was last received during log consolidation. This field is case-insensitive, and allows the use of wildcards (\* and ?). To enter multiple values, separate them with a semicolon (;).
  - **From, To** - The time range settings to filter events by time they were last received from the remote server during log consolidation.

For each time range, the following settings are available:

- **From** - The beginning of the time range. Possible values:
  - **First Record** - Filter starting with the earliest date and time in the respective log field.
  - **Records On** - Filter starting with a particular date and time.
- **To** - The end of the time range. Possible values:
  - **Last Record** - Filter ending with the latest date and time in the respective log field.
  - **Records On** - Filter ending with a particular date and time.

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.

- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

# DeviceLock Reports

## Report Categories and Types

DeviceLock lets you create reports using data from logs stored on DeviceLock Enterprise Server. Use reports to arrange and display statistical data on a user's device- and protocol-related activities in a separate file. When generating a report, you can define report parameters to filter the data and display the information that is relevant to you. For example, you can specify the start and end date and time of the report period for which data is displayed.

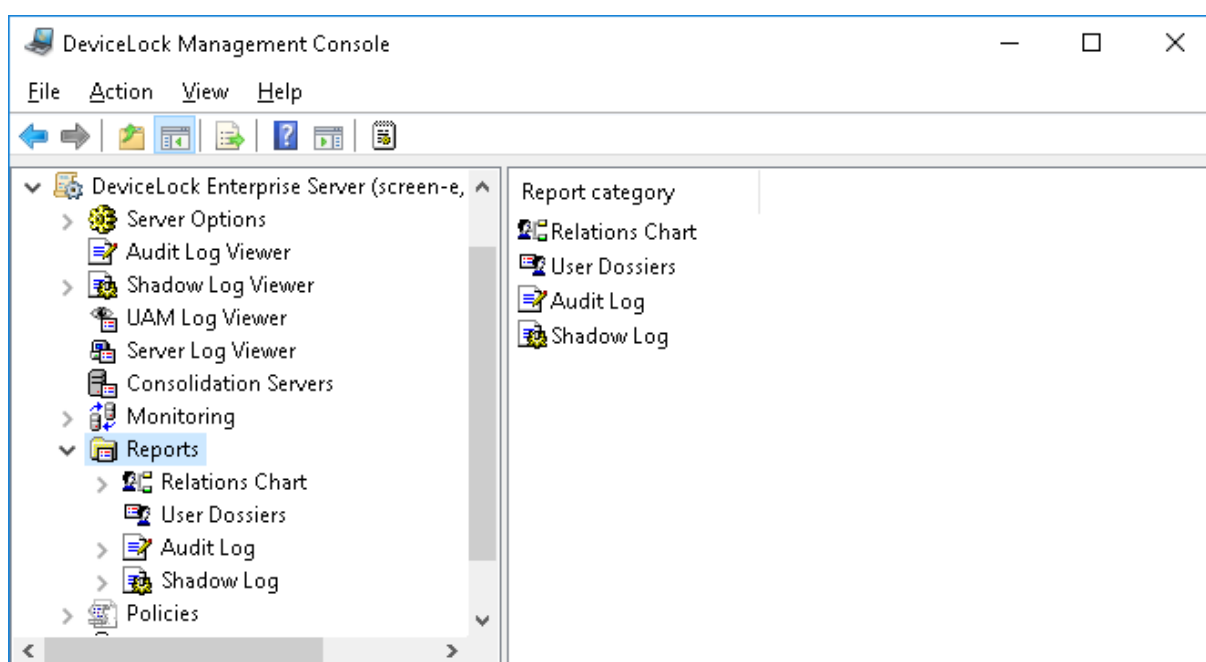
You can also create highly visual and interactive reports (relationship graphs) to show and analyze connections of your organization's employees based on frequency and channels of communication. Graphs let you visually analyze who interacts with whom, how frequently, and in what way their communications take place.

Reports can be created, automatically sent to you via e-mail, stored, exported to a variety of formats and shared with others. Reports are created by using DeviceLock Management Console.

DeviceLock provides reports of the following categories:

- [Relations Charts](#) are interactive reports that analyze interactions of people throughout your organization and create visual linkages between them based on frequency and channels of communication.
- [User Dossiers](#) enable authorized persons to keep track of computer user activity by using a convenient graphical representation of user action statistics. User dossiers provide statistical indicators to monitor and assess various aspects of users' behavior, such as frequency of attempts to perform unauthorized actions or transfer large volumes of data, changes in user online activity, etc.
- [Audit Log Reports](#) are based on data from the audit log files collected by DeviceLock Enterprise Server. Only reports of predefined types can be created. Report types cannot be modified nor can new (custom) report types be created.
- [Shadow Log Reports](#) are based on data from the shadow log files collected by DeviceLock Enterprise Server. They contain the combined data from the shadow log and deleted shadow data log. Only reports of predefined types can be created. Report types cannot be modified nor can new (custom) report types be created.

These report categories are displayed in the console tree, under **DeviceLock Enterprise Server > Reports**.



The shortcut menu on the **Reports** node provides the following commands:

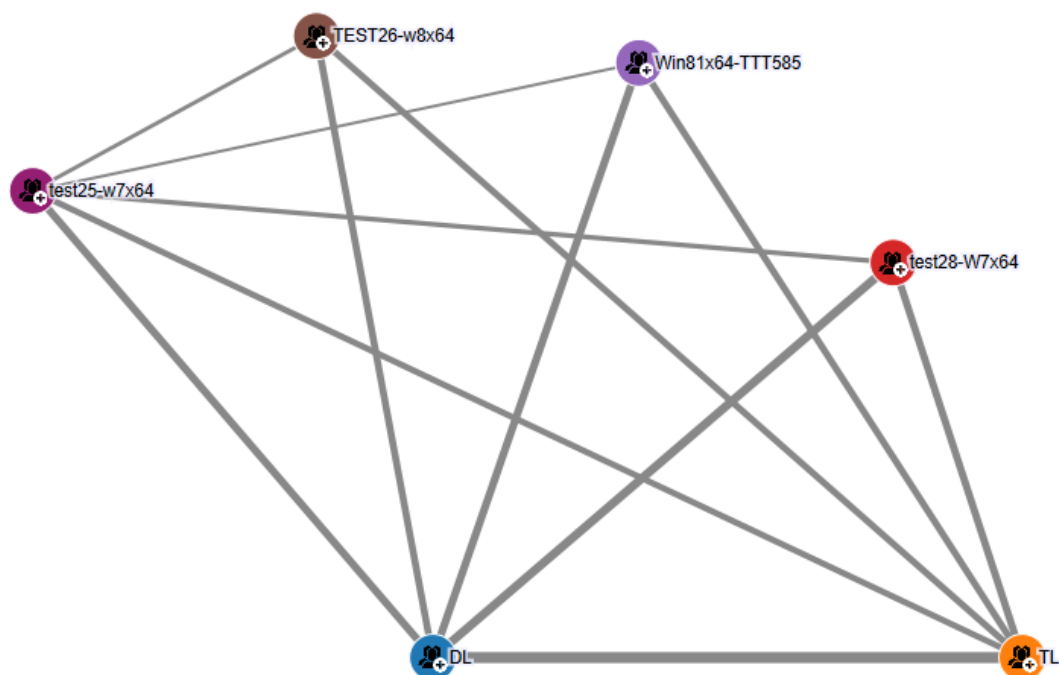
- **Notification Settings** - Allows you to configure e-mail delivery of reports (except for User Dossiers and Relations Charts). To deliver reports by e-mail, you should specify SMTP server settings and recipient addresses. For details, see [Configuring E-mail Delivery of Reports](#).
- **Set Default Format** - Allows you to specify the report output format to use for reports. The available options are HTML, PDF (default option) and RTF. Setting a report format does not affect Relations Charts and User Dossiers. For details, see [Setting Default Format for Reports](#).

## Relations Charts

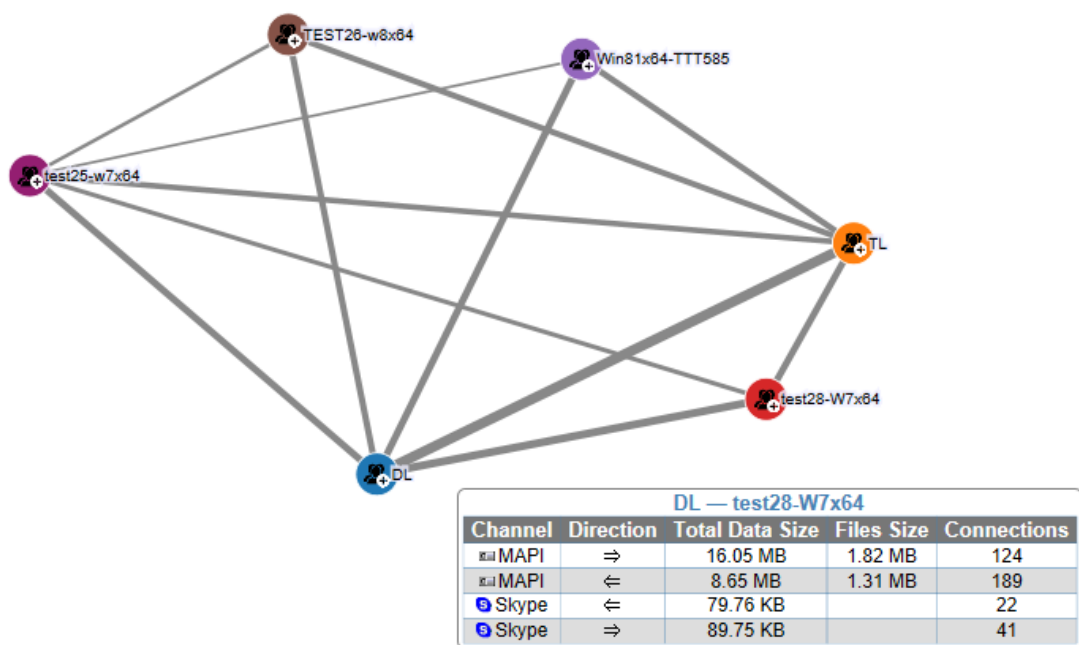
Relations charts let you explore statistical data on a user's protocol-related activities through interactive graphical visualizations of data collected into audit and shadow logs, including the deleted shadow data log. These reports are displayed in the form of graphs. Graphs use data types such as instant messenger chats, files transferred through instant messengers, calls, social network chats, e-mail messages and attachments, and are generated for the following protocols: IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMTP, Social Networks, Telegram, Viber, Web Mail, WhatsApp, and Zoom. However, relations charts may not reflect deleted shadow data specific to the size of file transferred through instant messengers and e-mail attachments.

Graphs are composed of two main components: nodes (participants) and lines. A node represents an Active Directory (AD) object, such as a domain, an organizational unit (OU), or a user. A line represents a connection or relationship between two nodes. Connections between two nodes (participants) are calculated based on the total number of instant messenger chats, files transferred through instant messengers, calls, social network chats, e-mail messages, and e-mail attachments between them. Thin lines indicate a weak communication relationship, while thick lines represent a strong communication relationship.

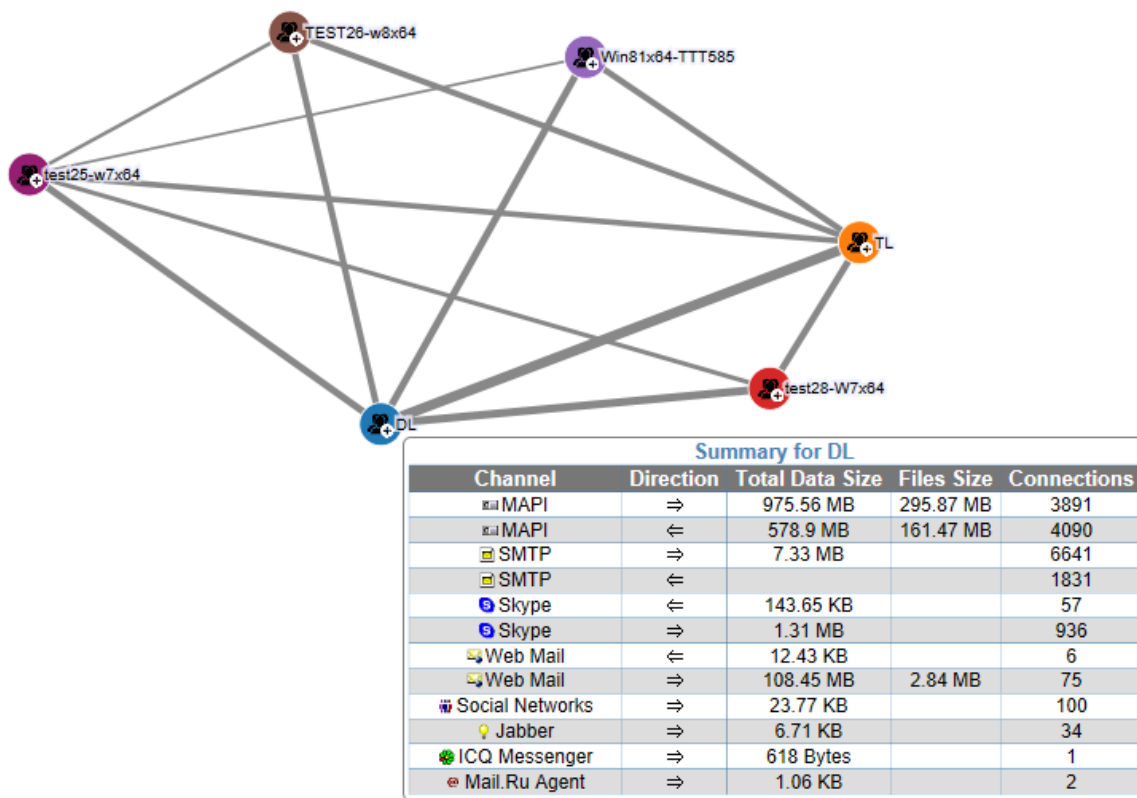




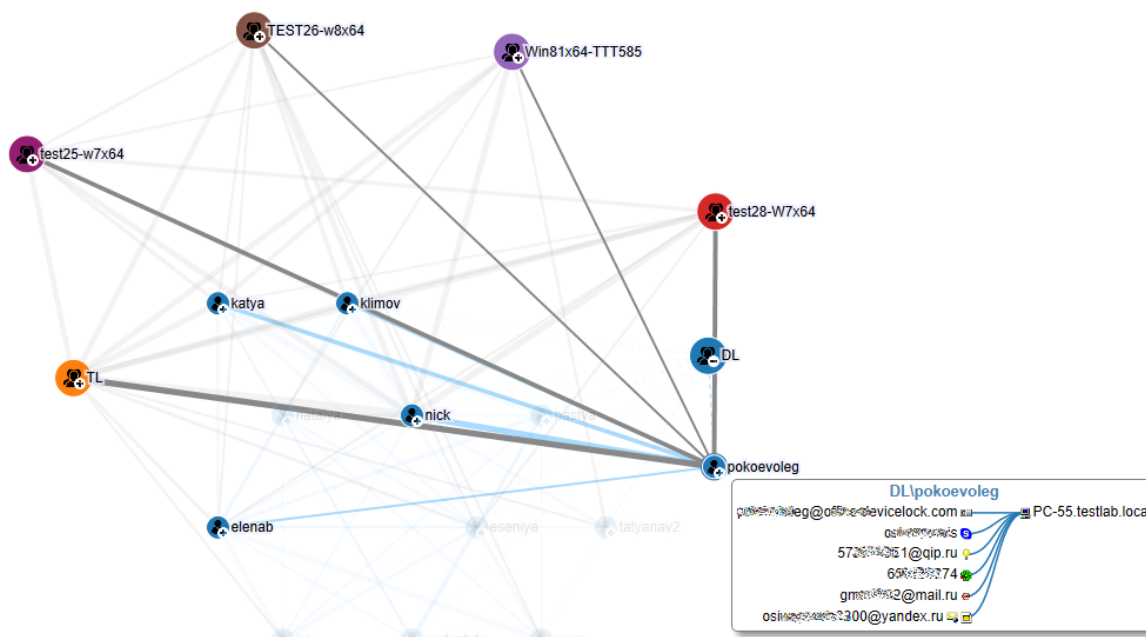
When you point to a line, a pop-up window displays information about a relationship between the connected nodes. This information includes a communication channel (for example, Skype, MAPI), the direction of communication (incoming/outgoing), the total size of the data and files transferred, and the number of connections (such as instant messenger chats, files transferred through an instant messenger, Skype calls, social network chats, e-mail messages, and e-mail attachments) per channel.



Graphs use a hierarchical structure. The top-level nodes represent your organization's domains. All top-level nodes have different colors. Clicking the plus sign (+) at the bottom right corner of a top-level node displays lower-level nodes representing users that are members of this domain. All lower-level nodes have the same color as the respective top-level node, making it easy to visually identify users from the same domain. Clicking the plus sign (+) at the bottom right corner of a user node displays this user's identifiers (such as e-mail addresses, social network and instant messenger IDs) and connections with other users. When a node is expanded, clicking the minus sign (-) collapses it.



When you point to a user's node, a pop-up window displays information about this user. This information includes the user's name in the following format: *DOMAIN\UserName* (for example, *DL\katya*), the name(s) of the user's computer(s), and the user's identifiers (such as e-mail addresses, social network and instant messenger IDs).



There are two types of users: internal and external. Internal users are inside the corporate network and are members of your organization's domain, while external users are outside the corporate network and are not members of your organization's domain. External users are identified by e-mail addresses, social network IDs, and instant messenger IDs.

## Domain and User Statistics

Pointing to a report item may pop up more information about that item. This capability is available for lines and user nodes as described earlier in this section. A pop-up box containing additional information also appears when you:

- Point to a domain node (see [Domain Statistics](#))
- Expand a user node, and then point to any of the user's identifiers (see [User ID Statistics](#))
- Point to a **Unique** node (see [Unique Contact Statistics](#))

### Domain Statistics

When you point to the node representing a certain domain, the report pops up summary information about the load of communication channels caused by all domain users. The pop-up box displays the domain name, lists the communication channels, and provides the following information on each channel:

- **Channel** - Indicates the communication protocol, such as Skype, MAPI, SMTP, Web Mail, ICQ Messenger, and so forth.
- **Direction** - Indicates the direction of communication:
  - Rightwards arrow ( $\Rightarrow$ ) denotes communication from domain users to external users.
  - Leftwards arrow ( $\Leftarrow$ ) denotes communication from external users to domain users.
  - Bidirectional arrow ( $\Leftrightarrow$ ) denotes communication between domain users.

- **Total Data Size** - The total volume of data transferred by all domain users through the specified channel in the specified direction.
- **Files Size** - The total size of the files transferred by all domain users through the specified channel in the specified direction.
- **Connections** - The total number of connections using the specified channel in the specified direction that were made by all domain users.

## User ID Statistics

When you expand the node representing a certain user, and then point to a user identifier (such as an e-mail address or an instant messenger ID) under the user node, the report pops up summary information about the total load of the communication channels caused by that user identifier.

The heading of the pop-up box that appears is composed of the selected user identifier followed by a list of user identifiers that communicated with that user identifier:

- In case of an internal user identifier, the list includes no more than 3 user identifiers. Ellipsis indicates that the list includes not all identifiers.
- In case of an external user identifier, the list includes no more than 5 domain user names. Ellipsis indicates that the list includes not all user names.

The pop-up box lists the communication channels, and displays the following information about each channel:

- **Channel** - Indicates the communication protocol, such as Skype, MAPI, SMTP, Web Mail, ICQ Messenger, and so forth.
- **Direction** - Indicates the direction of communication:
  - Rightwards arrow (⇒) denotes communication to other users, both internal and external.
  - Leftwards arrow (⇐) denotes communication from other users, both internal and external.
- **Total Data Size** - The total volume of data transferred by the given user identifier through the specified channel in the specified direction.
- **Files Size** - The total size of the files transferred by the given user identifier through the specified channel in the specified direction.
- **Connections** - The total number of connections made by the given user identifier through the specified channel in the specified direction.

The pop-up box provides information about all communications of the given identifier even if that identifier applies to multiple communication protocols. However, the data volume, files size and number of connections are calculated for each identifier separately. The values displayed for each protocol are specific to the given identifier even if the user has multiple identifiers for that protocol.

## Unique Contact Statistics

When you point to the **Unique** node of a certain internal user, the report pops up summary information about the load of the communication channels caused by all unique contacts of that

user. The pop-up box displays the domain user name, lists the communication channels, and provides the following information on each channel:

- **Channel** - Indicates the communication protocol, such as Skype, MAPI, SMTP, Web Mail, ICQ Messenger, and so forth.
- **Direction** - Indicates the direction of communication:
  - Rightwards arrow ( $\Rightarrow$ ) denotes communication to the user's unique contacts.
  - Leftwards arrow ( $\Leftarrow$ ) denotes communication from the user's unique contacts.
- **Total Data Size** - The total volume of data transferred by the user's unique contacts through the specified channel in the specified direction.
- **Files Size** - The total size of the files transferred by the user's unique contacts through the specified channel in the specified direction.
- **Connections** - The total number of connections using the specified channel in the specified direction that were made by the user's unique contacts.

## Interacting with a Graph

Interacting with a graph involves the following:

- **Zooming in and out.** You can change the way a graph is displayed by using the zoom function. To zoom in or out, do one of the following:
  - Rotate the mouse wheel backward or forward.
  - Press and hold the Ctrl key, and then press the plus (+) or minus (-) key.
- **Selecting one or more nodes in a graph.** You can change the display of a graph to show only selected nodes for further selective analysis on graph data. If nodes are selected, then only those nodes and nodes directly connected to selected nodes are displayed. Unselected nodes become inactive (grayed out). You can select one or more graph nodes by clicking while holding down the Ctrl key.
- **Moving one or more nodes in a graph.** You can move any node in a graph to a less-occupied section of the screen, while maintaining all its connections (links). To move the selected node, select and drag the node to the desired location.
- **Grouping unique contacts.** A unique contact is an external user that communicates with one and only one internal user. If desired, you can group together unique contacts (if any) that internal users communicate with. To group all unique contacts for each internal user, right-click the graph, and then click **Group unique contacts**. The identifiers of the unique contacts (e-mail addresses, social network, and instant messenger IDs) will be placed inside the **Unique** node for each internal user. The grouping method will help you quickly and easily find unique contacts. When unique contacts are grouped, applying the **Group unique contacts** command removes the grouping. As unique contacts are grouped together by default, the first use of that command ungroups the unique contacts. Apply that command once more to restore the grouping of unique contacts.
- **Setting a limit for displaying users per one click on a node.** You can control how many users are shown in a graph each time when the plus sign (+) on a node is clicked. To configure the

number of users to display per one click on a node, right-click in the graph, and then click **Populate contacts/users threshold**. In the dialog box that opens, select the **Populate contacts/users threshold** check box, and then, in the **Threshold** box, type or select the number of users (the default is **20** users). When the threshold is specified, the most communicatively active contacts on the user's contact list are displayed first. Clicking the plus sign (+) in the top left corner of a user node displays all the user's remaining contacts. Clicking the minus sign (-) in the bottom right corner of a user node collapses the previously opened user's contacts. The limit for displaying users is also applicable to the nodes that represent domains and the **Unique** nodes. To view the full list, click the plus sign (+) in the top left corner of the node. To return to the limited list, click the minus sign (-) in the bottom right corner of the node.

## Relations Chart Node

Relations Charts are created by tasks listed in the console under **DeviceLock Enterprise Server > Reports > Relations Chart**. When such a task is selected in the console tree, the details pane lists the Relations Charts created by that task. For further details, see [Report Creation Tasks](#).

The shortcut menu on the **Relations Chart** node provides the following commands:

- **Create Task** - Configures a new task of creating Relations Charts. Task settings are entered in the dialog boxes that appear.
- **Refresh** - Updates the list of tasks with the latest information.

For details on this category of reports, see [Relations Charts](#).

## Relations Chart Report

Expand the node that represents a Relations Chart creation task (see [Report Creation Tasks](#)) to view Relations Charts created by that task. The details pane displays the Relations Chart you have selected in the console tree. For details on this category of reports, see [Relations Charts](#).

When you select a Relations Chart creation task in the console tree, the details pane lists the task's reports (Relations Charts). For details on the list of reports, see [Viewing Reports Created by a Task](#).

The shortcut menu on a Relations Chart provides the following commands:

- **Open** - Displays the Relations Chart in the details pane. The Relations Chart can also be displayed by selecting it in the console tree.
- **Rename** - Changes the name of the selected Relations Chart.
- **View parameters** - Opens the dialog box to view the report parameters specified for that Relations Chart.
- **Delete** - Deletes the selected Relations Chart.
- **Refresh** - Updates the Relations Chart in the details pane.

## User Dossiers

User dossiers is a powerful and easy-to-use solution that enables authorized persons to keep track of computer user activity by using a convenient graphical representation of user action statistics.

The statistical overview of online user activity presented in User Dossiers is based upon various indicators that are enriched with LDAP-compatible directory data (including Active Directory Domain Services). User Dossiers show the frequency of attempts to perform unauthorized actions, transfer large amounts of data, reveal changes in the network user activity, and so forth. The statistical data provided by User Dossiers assists Administrators in analyzing the history of user activity and helps identify typical violations of security policies. Graphical visualization of statistics gives a convenient way to reveal most active users.

User dossiers provide statistical indicators to monitor and assess various aspects of users' behavior, such as frequency of attempts to perform unauthorized actions or transfer large volumes of data, changes in user online activity, etc. With these indicators, user dossiers make user activity more transparent, and improve the monitoring of users' actions from an information security standpoint.

User dossiers constitute a single directory that covers all statistics of user activity registered by the DeviceLock Service. The statistical data accumulates in the database of the DeviceLock Enterprise Server, and is retrieved when needed to represent in user dossiers. Statistics are replenished as new data appears in DeviceLock logs on the server. Statistics in user dossiers updates automatically during low server load, as well as on a schedule.

To display additional information about users, a connection to Active Directory Domain Services or another LDAP-compatible directory service can be configured. The DeviceLock Enterprise Server gets user account information from the directory service, and adds it to user dossiers. Removing users from the directory service does not delete their dossiers.

User dossiers are based on audit and shadow logs stored on the DeviceLock Enterprise Server. However, deleting log records does not cause the loss of data already registered in the user dossier. Having been registered in the dossier, the statistical data on user activity no longer depends on the logs from which it was derived as user dossiers are stored separately from the logs.

User dossier data is built upon the records in the shadow log and audit log. Primarily, shadow log records are used, and then they are supplemented with the data from the audit log. To provide meaningful user dossier data, shadow copying must be configured.

## Event folding

When building user dossiers, records of certain events that occurred over a certain threshold period are combined into a single event. This feature, known as event folding, optimizes the processing of event data and improves the accuracy of user dossiers. The threshold period is 10 seconds.

Given that a single user action often causes multiple events, DeviceLock applies event folding when processing events from the audit log. Events of the same type such as Access Allowed or Access Denied are combined into one event if all of the following conditions are met:

- The time difference between events is no more than 10 seconds.
- The event records have the same values of the following fields: Server, Computer, User, Source, Event, PID, Process, Name, Information.

Event folding is performed when building any diagrams, charts, and lists on user cards.

## Getting started with user dossiers

The administrator can view user dossiers in the DeviceLock Management Console details pane, having selected **DeviceLock Enterprise Server > Reports > User Dossiers** in the console tree. When displaying user dossiers, the details pane splits in two areas:

- **User List** - On the left is a list of users and groups, received from the DeviceLock Enterprise Server.
- **User Card** - The card of the user selected from the list on the left is displayed on the right. The card shows the user's account information along with statistics on the user's actions as registered in DeviceLock Enterprise Server logs.

User dossiers are based on information held in DeviceLock Enterprise Server log records. Additional information to display on user cards can be retrieved from directory services (see [Directory Service Connection Settings](#)).

## User List

The user list shows the names of users and groups. Groups are represented as containers that hold group member users. Each group can be expanded to view a list of users it holds.

The list initially contains only built-in groups from the DeviceLock Enterprise Server, such as the **All** built-in group that holds all users found in the DeviceLock Enterprise Server logs. Administrators can create custom groups, and add users to such groups at their discretion. A user can be added to multiple groups.

The following controls are provided for managing the user list:

- Above the list is the quick search box for searching users by name (such as by first name, last name, or user account name). Enter a name in the quick search box to find users with that name.
- Groups in the list are expandable. Double-click the name of the group to view the users it holds. Then, click a user name to open their card.
- On each group, a shortcut menu is available. Right-click a group name, and then use the following shortcut menu commands:
  - **Create** - Creating a custom group.  
Custom groups can be instrumental in analyzing statistics of users with similar profiles. A good practice is to combine such users into groups.
  - **Rename** - Renaming the group.  
This command is unavailable on built-in groups, such as the **All** group. Built-in group names are determined by the server. Manually changing them is not allowed.
  - **Paste** - Adding a user from the Clipboard to the group. To use this command, first use the **Copy** command to copy the user onto the Clipboard.  
This command is unavailable on built-in groups, such as the **All** group. Built-in group membership is determined by the server. Changing it manually is not allowed.



- **Delete** - Deleting the group. This command does not delete users that were members of the group.  
This command is unavailable on built-in groups, such as the **All** group. Deletion of built-in groups is not allowed.
- On each user, a shortcut menu is available. Right-click a user name, and then use the following shortcut menu commands:
  - **Copy** - Copying the user onto the Clipboard. Use this command in conjunction with the **Paste** command from the group menu to add users to custom groups.
  - **Delete** - Removing the user from membership in the custom group. This command does not delete the user itself.  
This command is unavailable for users in built-in groups, such as the **All** group. Built-in group membership is determined by the server. Changing it manually is not allowed.

## User Card

In the user list, each group can be expanded to view the users - members of that group. Next to the list is displayed the card of the user selected in that list.

The top area of the card is composed of the following elements:

- [User account information](#)
- [User loyalty indicator](#)
- [User activity overview](#)

After the overview of user activity, the card presents statistics of devices and protocols usage by the given user. This part of the card includes the following elements:

- [Reporting period selector](#)
- [User activity charts](#)
- [User action details](#)
- [Relations chart](#)

The user card provides a shortcut menu that enables copying text to the Clipboard. To copy text, select it on the user card and press **Ctrl+C**, or right-click the selected text, and then click **Copy**.

### User account information

At the top of the card, the user image (photo) is displayed, if it was obtained from the directory service; otherwise, a generic user icon is displayed.

Next to the user photo, the card displays information about this user received from the directory service, including a list of directory groups of which this user is a member (the **Member of** field). Then the card lists the DeviceLock Enterprise Server's custom groups to which this user belongs (the **Groups** field), and all accounts of this user that are registered in the logs on the DeviceLock Enterprise Server (the **Accounts** field).

Thus, the following information from Active Directory is displayed on an Active Directory domain user card:

- User photo (photo)
- Display name (displayName)
- Description (description)
- Department (department)
- E-mail addresses (mail)
- Mobile phone number (mobile)
- Manager name (manager)
- Office location (physicalDeliveryOfficeName)
- Active Directory groups of which this user is a member (memberOf)

The card lists the accounts that this user used to access network resources (protocols), such as web mail, instant messaging, etc. Each account displays its name and protocol icon. To view the name of the protocol, hover over the protocol icon.

---

**Note**

Instead of user accounts for social networks, the card lists the names of the social networks that this user accessed.

---

### User loyalty indicator

The card displays a number of indicators summarizing the statistics of user actions for the reporting period in order to identify anomalies or suspicious activity. These indicators constitute an indicator of user loyalty (normality). The loyalty indicator helps detect suspicious user activity and anomalies by indicating deviation of user behavior from a well-determined baseline.



The user activity baseline is determined as the average level of the user's activity for a certain period preceding the reporting period. The duration of this baseline period varies depending upon the reporting period. The indicator compares the average levels of activity during the reporting period with the baseline to identify changes to user behavior, and to determine whether they are acting typically (the indicator is closer to 100%) or abnormally (the indicator is closer to 0%). Possible options for the reporting period: the last 7, 30, or 365 days before the current date.

The duration of the period on which the user activity baseline is determined varies depending upon the selected reporting period:

Reporting period	Baseline period
Last 7 days	Either 12 valid 7-day intervals before the reporting period, or all days registered in the logs before the reporting period if less than 12 such 7-day intervals are registered.
Last 30 days	Either 12 valid 30-day intervals before the reporting period, or all days registered in the logs before the reporting period if less than 12 such 30-day intervals are registered.
Last 365 days	Either 2 valid 365-day intervals before the reporting period, or all days registered in the logs before the reporting period if less than 2 such 365-day intervals are registered.

Only intervals with nonzero user activity are considered valid. For the 7- and 30-day reporting periods, the search for such intervals is limited to the last year before the reporting period. If no valid intervals can be found for the baseline period or no user activity has been registered for the reporting period, the indicator displays “Insufficient data”.

To determine the activity levels, the indicator determines the average numbers of actions that were denied and allowed by the DeviceLock Service, and then it calculates the percentage and direction of changes in these numbers compared to the baseline. The overall result is displayed on the loyalty indicator, characterizing changes in the current activity level compared to the baseline. A higher overall result indicates better compliance with the DeviceLock security policies.

The indicator is complemented by a dashed hand showing the group’s average value, which provides the ability to compare the user’s personal loyalty index to the average index of their coworkers group. For further details, see [Group average loyalty index](#).

The loyalty indicator also includes refinement indicators that specify the contribution of different types of user activity to the change in the overall result:

- Allow Read - The allowed attempts to receive data.
- Allow Write - The allowed attempts to send data.
- Deny Read - The denied attempts to receive data.
- Deny Write - The denied attempts to send data.
- Career Search - The attempts to use job search websites.

A refinement indicator is displayed only if the level of the respective user activity has changed. Thus, the Career Search indicator appears when there is a change in the level of activity associated with the use of job search websites. The Allow Read/Write or Deny Read/Write indicators appear when the average number of allowed or denied data exchange attempts has changed.

For each of the refinement indicators (except for Career Search), the following notation is used for how it changed in the reporting period compared to the baseline:

- Up arrow, red - An increase in the number of allowed or denied attempts.
- Down arrow, green - A decrease in the number of allowed or denied attempts.

- Vertical bar, red - A constant non-zero number of allowed or denied attempts.
- Vertical bar, green - A constant number of allowed attempts and no denied attempts.
- Long dash, green - No allowed / denied attempts, which led to an increase in the overall loyalty indicator.

### ***Group average loyalty index***

In addition to the user's personal loyalty index, the indicator presents the average loyalty index for the group of which this user is a member. The group average index is an average of the loyalty indexes for the group member users. When calculating the group average, the boundary values of the source data are truncated to prevent distortion due to the highest and lowest indexes.

The group average serves to compare the user's personal loyalty index to the average index of their coworkers group. An abnormal deviation of the personal loyalty index from the group's average may indicate a suspicious user activity. This is the case, for example, when the group average is in the green area whereas the user's loyalty index is not.

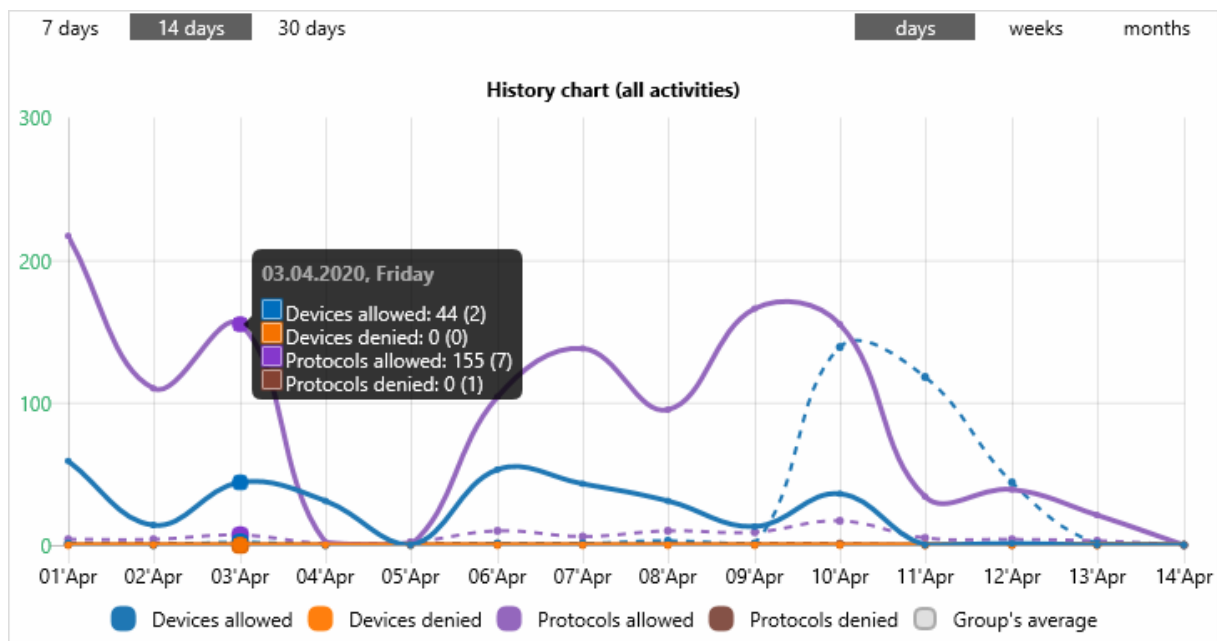
The group average is shown by a dashed hand in the same diagram as the user's loyalty indicator. This design helps to compare the current user's personal index with the group average.

The group average value depends upon the group in which the user is selected. Note that in order to select a user, you must first expand a group, and then select a user from that group. The indicator displays the average for the group from which the user is selected.

Since the user can be a member of multiple groups, the group's average value may vary depending upon how the user is selected. For example, if a user is selected from the list of members of the built-in group **All**, the group's average value is the average by all users registered with the server's logs. If you select a user from the list of members of a custom group, the group's average value is the average by the member users of that group.

### **User activity overview**

The card displays a graph entitled **History chart (all activities)** that provides an overview of user activity for a certain period.



One can choose from the following periods:

- Days - Last 7, 14, or 30 days, including the current day. Each day is represented by a marker of its date on the horizontal axis, above which the graph displays the total readings for that day.
- Weeks - Last 4, 8, or 12 weeks, including the current week. Each week is represented by a marker of its start-end dates on the horizontal axis, above which the graph displays the total readings for that week.
- Months - 12 monthly intervals preceding the current date. Each interval is represented by a marker of its end date on the horizontal axis, above which the graph displays the total readings for that interval.

This graph provides an insight into user's actions for the selected period, with a detailing of down to one day. It displays several curves representing the number of allowed and denied user actions:

- Devices allowed - The number of allowed attempts to access devices.
- Devices denied - The number of denied attempts to access devices.
- Protocols allowed - The number of allowed attempts to access protocols.
- Protocols denied - The number of denied attempts to access protocols.

To view numeric readings, hover your mouse over a curve above a marker. A pop-up window will appear that indicates the selected marker (the day, week, or month), and also displays the numbers of allowed and denied user actions for the time corresponding to this marker. The values in parentheses indicate the average number of actions for the group in which the user is selected (see [Group averages](#)).

By default, the graph displays all curves. To hide a curve, click its identifier below the graph. For example, if you are interested in only "denied" curves, you can hide the "allowed" curves by clicking their identifiers. To display the curve again, click its identifier once more.

Each curve in the graph is complemented by a dashed curve representing the [group averages](#). When a main curve is hidden, its complementary average curve is not displayed as well.

### **Group averages**

In addition to the number of actions of the selected user, the history chart also displays the average values for the group of which this user is a member. Each of these group averages is an average number of respective actions by the group members (an average number of allowed / denied attempts to access devices / protocols). When calculating a group average, the boundary values of the source data are truncated to prevent distortion due to the highest and lowest values in the group.

The group averages serve to compare the user's activity metrics to those of their coworkers group. Abnormal deviations from the average metrics may indicate suspicious user actions. This is the case, for example, when the number of the user's denied actions is substantially higher than the respective group average.

Group averages are indicated by dashed lines of the corresponding color. For example, the average number of denied attempts to access devices is indicated by a dashed line of the same color as the curve representing the number of the user's denied attempts to access devices. This design makes it easier to compare user metrics to their group averages.

If you are not interested in averages, click the **Group's average** label below the graph to hide this information. To display the averages again, click this label once more.

The group averages depend upon the group in which the user is selected. Note that in order to select a user, you must first expand a group, and then select a user from that group. The graph displays the averages for the group that is used for selection.

Since the user can be a member of multiple groups, group averages may vary depending upon how the user is selected. For example, if a user is selected from the list of members of the built-in group **All**, the averages are calculated for all users registered with the server's logs. If you select a user from the list of members of a custom group, the averages are calculated only for the member users of that group.

### **Reporting period selector**

The card displays statistics on user actions for the selected reporting period. The date range of the reporting period determines the dates of events to include in the statistics. User action statistics are based on the log data on events that occurred in the reporting period.

The selector of the reporting period is at the top of the statistics display area. One can select a predefined date range or use a custom range. The following predefined date ranges are available:

- Today - The current date.
- Yesterday - The date preceding the current date.
- Last week - The date range from the first to the last day of the previous calendar week.
- Last month - The date range from the first to the last day of the previous calendar month.

- Last 7 days - The date range spans 7 days preceding the current date.
- Last 30 days - The date range spans 30 days preceding the current date.

Using custom date range, one can select:

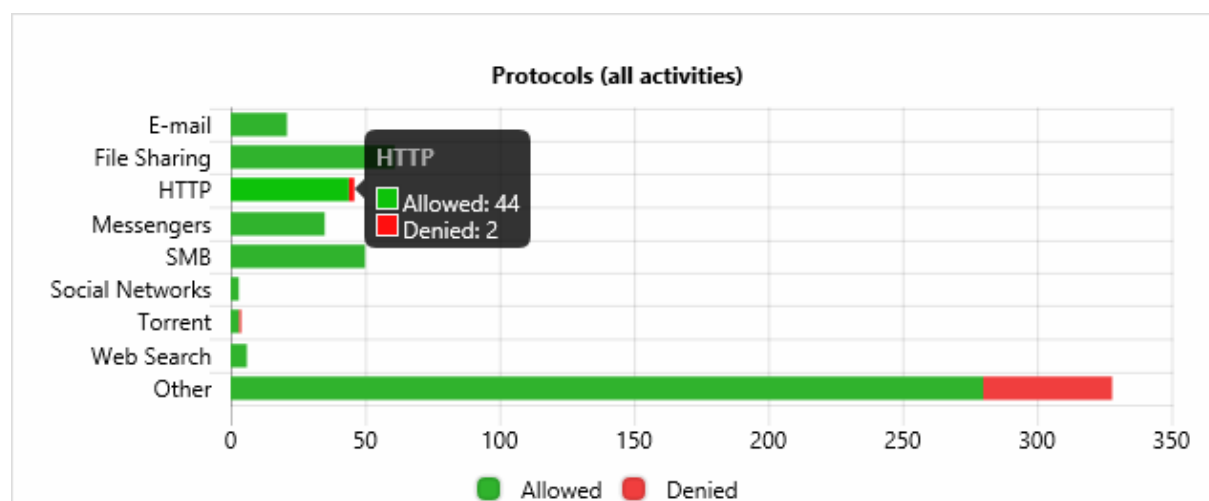
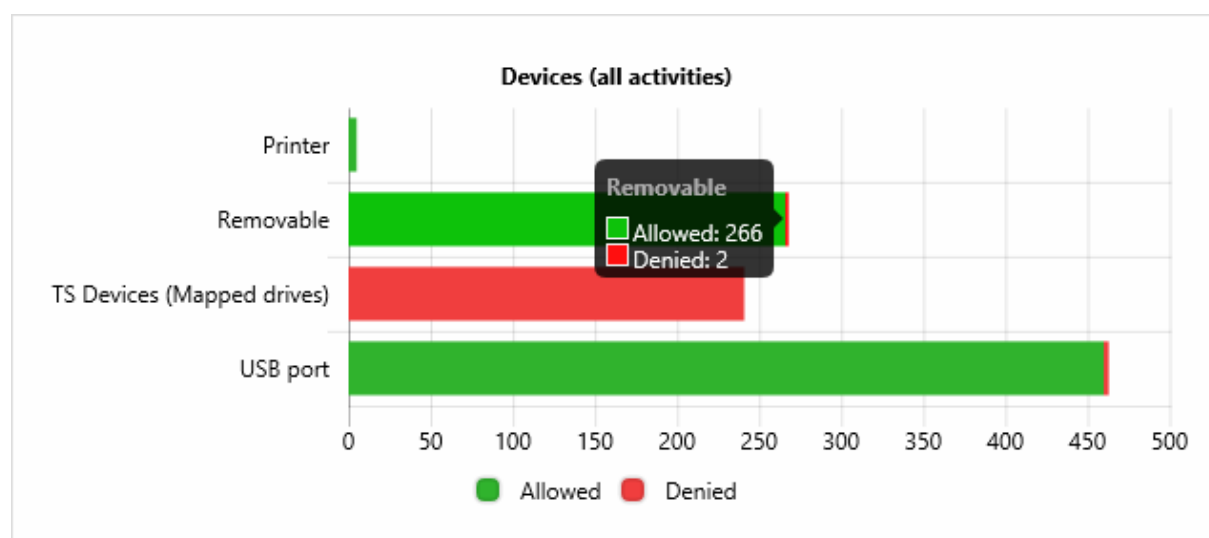
- A single date - Click the desired date to select.
- A continuous range of dates - Click the start date and then click the end date of the desired date range.
- All days of a certain month - Click the name of the month at the top of the selector.

Having selected the desired date range, click **OK** to apply your changes to the reporting period.

To quickly switch the reporting period, use the commands next to the date range selector. Click **Backward** or **Forward** to move the reporting period back or forward in time. For example, if you select a range of one week, these commands move the reporting period back one week or one week forward, respectively.

## User activity charts

The statistics area starts with two bar-charts representing a breakdown of the number of allowed and denied user actions by device types - entitled **Devices (all activities)**, and by protocols - entitled **Protocols (all activities)**. The charts use horizontal bars to show the number of actions.



Each bar in the chart indicates the total number of allowed and denied user actions for a particular data transmission channel (device type or protocol). The Tor Browser bar indicates the number of attempts to connect to the Tor network denied by the “Block Tor Browser traffic” security setting.

In the protocols chart, some bars aggregate actions by multiple channels:

- **E-mail** - Protocols such as SMTP, MAPI, IBM Notes, or Web Mail.
- **Messengers** - Instant messaging protocols such as Skype, Jabber, Telegram, WhatsApp, Viber, etc.
- **Proxy** - HTTP / SOCKS4 / SOCKS5 proxy servers. Aggregates the actions denied by the “Block proxy traffic” security setting.
- **Other** - Unidentified protocol types. Aggregates the actions logged by Protocols White List rules for Any or SSL protocol and/or Basic IP Firewall rules. This bar also counts the actions denied by the “Block unrecognized outgoing SSL traffic” security setting.

Hover over such an “aggregate” bar to view the number of actions for each channel.

The other bars correspond to individual device types / protocols. The charts display only the bars corresponding to the devices and protocols for which any user actions were logged.

The bar is divided into two segments: the green segment represents allowed actions while the red one stands for denied actions. The length of the green segment indicates the number of allowed actions; the length of the entire bar indicates the total number of actions, both allowed and denied. To view numeric readings, hover over a bar. A pop-up window will appear that indicates the device type or protocol corresponding to the selected bar, and also displays the numbers of user actions that were allowed or denied for this device type or protocol within the reporting period.

As some bars aggregate actions for multiple data transmission channels, on each of those bars a pop-up is provided for breaking down the number of actions by channel. The pop-up shows the channel names along with the number of allowed and denied user actions for each channel.

---

### Note

Unlike user dossiers that account for all events that were logged, DeviceLock reports may disregard some events. For instance, reports such as “Allowed & Denied access requests per channel” and “Read & Write access requests per device type” do not count the Insert and Remove events for USB devices. Therefore, the readings of the reports may differ from the readings of the history graph and activity charts in the user’s card.

---

## User action details

The user activity charts are followed by lists of files the user attempted to send, receive, or print (at most 10 files in each list). The contents of the lists depend upon which DeviceLock logs the files are registered in. For files registered in the Shadow log, the user card can list top largest files along with their size. For files that are registered in the Audit log, it can list the files that the user most frequently attempted to send, receive, or print, along with the number of attempts. The following file lists are provided:



- Top 10 types of incoming and outgoing files by file size - Two-column lists. The first column lists the file type descriptions. The second column displays the total size of the files of each type. Up to four lists can be displayed:

- **Top Allowed Incoming File types** - A list of file types that the user was allowed to receive.
- **Top Denied Incoming File types** - A list of file types that the user was not allowed to receive.
- **Top Allowed Outgoing File types** - A list of file types that the user was allowed to send.
- **Top Denied Outgoing File types** - A list of file types that the user was not allowed to send.

Each list includes up to 10 file types of the largest total file size. The lists are based on data from the Shadow log. If the log contains no data regarding a particular category of files (Allowed / Denied, Incoming / Outgoing), the card does not display the respective list(s).

- Top 10 incoming and outgoing files by file size or by number of attempts - Two-column lists. The first column lists the names of the files the user attempted to send or receive. The second column displays either the size of the file or the number of attempts to send or receive that file. Up to four lists can be displayed:

- **Top Allowed Incoming Files** - A list of files that the user was allowed to receive.
- **Top Denied Incoming Files** - A list of files that the user was not allowed to receive.
- **Top Allowed Outgoing Files** - A list of files that the user was allowed to send.
- **Top Denied Outgoing Files** - A list of files that the user was not allowed to send.

Each list includes up to 10 files of the largest size or up to 10 files with the largest number of attempts to send or receive. Lists showing file sizes are based on data from the Shadow log. Lists showing a number of attempts are based on data from the Audit log. If the log contains no data regarding a particular category of files (Allowed / Denied, Incoming / Outgoing), the card does not display the respective list(s).

To switch between viewing the list by file size / number of attempts, click the following item in the list header:

- Click **Show by Quantity** to view a list of files with the largest number of attempts.
- Click **Show by Size** to view a list of files of the largest size.

This switch is available if the Shadow log contains sufficient data to build the list of files. Otherwise, the files are listed by the number of send / receive attempts, and the items **Show by Quantity** and **Show by Size** are not displayed.

- Top 10 printed files by file size or by number of attempts - Two-column lists. The first column lists the names of the files the user attempted to print. The second column displays either the size of the file or the number of attempts to print that file. Up to two lists can be displayed:

- **Top Allowed Printed Files** - A list of files that the user was allowed to print.
- **Top Denied Printed Files** - A list of files that the user was not allowed to print.

Each list includes up to 10 files of the largest size or up to 10 files with the largest number of attempts to print. Lists showing file sizes are based on data from the Shadow log. Lists showing a number of attempts are based on data from the Audit log. If the log contains no data regarding a particular category of files (Allowed / Denied), the card does not display the respective list(s).

To switch between viewing the list by file size / number of attempts, click the following item in the list header:

- Click **Show by Quantity** to view a list of files with the largest number of attempts.
- Click **Show by Size** to view a list of files of the largest size.

This switch is available if the Shadow log contains sufficient data to build the list of files. Otherwise, the files are listed by the number of print attempts, and the items **Show by Quantity** and **Show by Size** are not displayed.

Next on the user card are two lists of rules that denied or allowed the transfer of certain content for this user / detected the transfer of content (Content-Aware Rules):

- **Top Allowed Content-Aware Rules** - The most frequently triggered rules that allowed or detected the transfer of content.
- **Top Denied Content-Aware Rules** - The most frequently triggered rules that denied the transfer of content.

The number of times each rule triggered is counted jointly for devices and protocols. Content detection rules are considered rules that allow the transfer of content.

The list includes up to 10 rules that triggered most frequently. For each rule, the list displays the name of the rule and the total number of times the rule triggered.

Then the user card provides information on the exchange of files and data with the user's contacts:

- **Top Contacts** - The contacts that the user most frequently exchanged files and data with. For each contact, the list provides the following information:
  - The name of the contact.
  - The total volume of data sent to or received from this contact. Displays only if the respective data exists in the Audit log and/or Shadow log.
  - The total size of files sent to or received from this contact. Displays only if the respective data exists in the Audit log and/or Shadow log.
  - The total number of communications with this contact.

The list includes up to 10 contacts with the largest number of communications.

## Relations chart

The statistics area completes with a chart that enables a review of interrelations and data exchange between the user and his contacts through graphical representation of DeviceLock's log data for the selected reporting period. This chart is built on data types such as instant messenger chats, files transferred through instant messengers, Skype calls, social network chats, e-mail messages and e-mail attachments. This takes into account the data transferred across various protocols, including IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMTP, Social Networks, Telegram, Viber, Web Mail, WhatsApp, and Zoom.

The chart appears in the form of a graph composed of two main components:

- Nodes - One of the nodes represents the user and the other nodes represent the user's contacts.
- Connection lines between nodes - Each line represents a relationship between the user and one of his contacts. Its thickness is proportional to the total number of user communications with the given contact.

When you point to a line, a pop-up window displays information about a relationship between the connected nodes. This information includes a communication channel (for example, Skype, MAPI), the direction of communication (incoming/outgoing), the total size of the data and files transferred, and the number of connections (such as instant messenger chats, files transferred through an instant messenger, Skype calls, social network chats, e-mail messages, and e-mail attachments) per channel.

When you point to a node, a pop-up window displays information about the user or contact. Depending upon the node type, this information may present the user or contact name, the name of the user's computer, and the identifiers of the user or contact (such as e-mail addresses, social network and instant messenger IDs).

For more on relations charts, see [Relations Charts](#).

## Directory Service Connection Settings

The menu on the **User Dossiers** node provides a command to configure a connection to an LDAP-compatible directory service, such as Active Directory or OpenLDAP. This connection extends user dossiers with information about users from the directory service (see [User account information](#)).

If there is no connection to a directory service, user dossiers are only based on information found in the DeviceLock Enterprise Server log records.

User dossiers automatically connect to Active Directory if the DeviceLock Enterprise Server computer is a member of an Active Directory domain. To access Active Directory, in this case, user dossiers by default use the DeviceLock Enterprise Server service's startup account specified by the [Log on as](#) parameter. If this account does not have sufficient rights to access Active Directory, credentials of an alternative account can be supplied in the directory service connection settings dialog box.

User dossiers retrieve updated information from the directory service on a daily basis at 1:00 AM local server time, as well as every time the DeviceLock Enterprise Server service starts.

### ***To manage directory service connection settings***

1. In the console tree, select **DeviceLock Enterprise Server > Reports > User Dossiers**.
2. Right-click **User Dossiers**, and select the **Directory Service Settings** command.
3. Set, view, or change the settings in the [Directory service connection settings dialog box](#) that appears.

## Directory service connection settings dialog box


The **Directory Service Settings** command brings up a dialog box to set, view, or change the settings to connect to an LDAP-compatible directory service. These settings depend upon the directory service selected:

- [Active Directory](#) - Credentials to access Active Directory domain services.
- [LDAP](#) - Credentials and other settings to connect to an LDAP server.

### Active Directory

Active Directory settings are used when the computer running the DeviceLock Enterprise Server is a member of an Active Directory domain, but the DeviceLock Enterprise Server service logon account does not have rights to access Active Directory. In this case, user dossiers can employ a domain user account with sufficient rights to retrieve data from Active Directory. It is also possible to connect to a specific Active Directory domain, which might be required when DeviceLock Enterprise Server runs on a computer that is not joined to a domain (stand-alone server), or user data needs to be retrieved from a different domain.

The dialog box provides the following fields to specify the Active Directory domain, and to supply the name and password of a domain user:

- **Host** - Either of the following:
  - The Fully Qualified Domain Name (FQDN) of the Active Directory domain.  
Example: production.company.com
  - The name or IP address of the server running the Active Directory domain controller.  
Example: dc1.production.company.comOne can select a domain controller from the list by clicking the  button next to this field.

---

#### Note

If no host is specified, user dossiers either connect to any available domain controller of the domain to which the DeviceLock Enterprise Server's computer is joined, or do not connect to Active Directory domain services (in the case of stand-alone server).

---

- **User Name** - The name of the domain user in either of the following formats:
  - user@domain - In this format, user is the user account name and domain is the domain UPN suffix.
  - domain\user - In this format, domain is the domain's short (NetBIOS) name and user is the domain user's logon name.
- **Password** - The password of the user account in the Active Directory domain.

---


#### Note

If no user name is specified, user dossiers access Active Directory with the DeviceLock Enterprise Server service's logon account specified by the [Log on as](#) parameter.

---

## LDAP

The dialog box provides the following fields to specify credentials and other settings to connect to an LDAP server (such as an OpenLDAP or AD LDS server):

- **Host** - The name or IP address of the LDAP server. One can select a server from the list by clicking the  button next to this field.
- **Port** - The LDAP server's TCP port number, 389 by default.
- **Base DN** - The starting point to search the directory tree. This must be a valid distinguished name (DN), such as `cn=users,o=company,c=US`. If the base DN is not specified, the search goes from the tree root. Click the **Fetch** button to select a naming context for the base DN.
- **User DN, Password** - The distinguished name (DN) and password of the directory user to access the LDAP server. User DN must be a valid DN, such as `cn=admin,o=company,c=US`.

---

### Note

If no user DN is specified, user dossiers access the LDAP server with the DeviceLock Enterprise Server service logon account specified by the [Log on as](#) parameter.

---

## Audit Log Reports

Audit Log reports are based on the data held in the DeviceLock Enterprise Server audit log files. The following report types are available in this category:

- [Allowed & Denied access requests per channel](#)
- [Allowed vs. Denied access requests](#)
- [Read & Write access requests per device type](#)
- [Top active computers](#)
- [Top active processes](#)
- [Top active users](#)
- [Top inserted USB & FireWire devices](#)
- [Top used USB devices](#)
- [DeviceLock Service versions](#)
- [DeviceLock Service versions by computers](#)
- [DeviceLock policy changes](#)
- [Top used Printers](#)
- [Top printed documents](#)
- [Top copied files by extension](#)

Under each report type, the console lists the tasks that create reports of that type. For instance, the tasks for creating "Top active computers" reports of the Audit Log category are listed in the console under **DeviceLock Enterprise Server > Reports > Audit Log > Top active computers**. When you select a task in the console tree, the details pane lists the reports created by that task. For further details, see [Report Creation Tasks](#).

## Allowed & Denied access requests per channel

This report shows the number of allowed and denied access requests per data transmission channel (devices and/or protocols).

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **User(s)** - Shows the users that were specified for the report.
- **Channel(s)** - Shows the data transmission channels that were selected for the report. The available options are: **all devices**, **all protocols**, and **all devices and protocols**.

---

### Note

- Reports for **all protocols** or **all devices and protocols** may contain the **Other** protocol record, which sums up access requests via unidentified protocol types logged by Protocols White List rules (**Any** or **SSL** protocol) and/or Basic IP Firewall rules.
  - When the **Block Tor Browser traffic** security setting is in effect, attempts to use the Tor Browser are accounted for as denied access requests via the **Other** protocol.
- 

The Report Results section contains a table and a chart that show detailed results of the report. The table has the following columns:

- **Channel** - Shows a data transmission channel.
- **Allowed** - Shows the number of allowed access requests.
- **Denied** - Shows the number of denied access requests.

## Allowed vs. Denied access requests

This report shows the total number of allowed and denied access requests sent through all data transmission channels (devices and/or protocols).

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header section contains the report title that appears at the very beginning of the report. The report title displays the report name.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **User(s)** - Shows the users that were specified for the report.
- **Channel(s)** - Shows the data transmission channels that were selected for the report. The available options are: **all devices**, **all protocols**, and **all devices and protocols**.

---

#### Note

- Reports for **all protocols** or **all devices and protocols** may contain the **Other** protocol record, which sums up access requests via unidentified protocol types logged by Protocols White List rules (**Any** or **SSL** protocol) and/or Basic IP Firewall rules.
  - When the **Block Tor Browser traffic** security setting is in effect, attempts to use the Tor Browser are accounted for as denied access requests via the **Other** protocol.
- 

The Report Results section contains a table and a pie chart that show detailed results of the report. The table has the following rows:

- **Allowed** - Shows the total number of allowed access requests and the respective percentage.
- **Denied** - Shows the total number of denied access requests and the respective percentage.
- **Total** - Shows the total number of all access requests and the respective percentage.

The pie chart represents the report results in percentages.

## Read & Write access requests per device type

This report shows the number of read and write access requests per device type. The report provides data only for the Floppy, iPhone, MTP, Optical Drive, Removable, TS Devices, Clipboard, Hard disk, Tape, Windows Mobile, and Palm device types.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Access Type(s)** - Shows the event types that were specified for the report.
- **Computer(s)** - Shows the computers that were specified for the report.
- **User(s)** - Shows the users that were specified for the report.

The Report Results section contains a table and a chart that show detailed results of the report. The table has the following columns:

- **Device Type** - Shows a device type.
- **Read** - Shows the number of read access requests.
- **Write** - Shows the number of write access requests.

The table also has a **Total** row that sums up all the values in the **Read** and **Write** columns.

## Top active computers

This report shows the most frequently used computers sorted according to the number of allowed and denied access requests. By default, the report lists the first 10 computers but you can specify any number of computers.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Channel(s)** - Shows the device types and/or protocols that were selected for the report.

---

### Note

- Reports with the **Other** protocol selected also count access requests via unidentified protocol types logged by Protocols White List rules (**Any** or **SSL** protocol) and Basic IP Firewall rules.
  - When the **Block Tor Browser traffic** security setting is in effect, reports with the **Other** protocol specified also count attempts to use the Tor Browser (considered as denied access requests via the **Other** protocol).
- 

The Report Results section contains two tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) computers having allowed access. Table 2 lists the top N (where N is a specific number) computers having denied access. These tables have the following columns:

- **Computer Name** - Shows a computer name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

## Top active processes

This report shows the most active processes (applications) sorted according to the number of allowed and denied access requests sent by each process. By default, the report lists the first 10



processes but you can specify any number of processes.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Channel(s)** - Shows the device types and/or protocols that were selected for the report.

---

#### Note

- Reports with the **Other** protocol selected also count access requests via unidentified protocol types logged by Protocols White List rules (**Any** or **SSL** protocol) and Basic IP Firewall rules.
  - When the **Block Tor Browser traffic** security setting is in effect, reports with the **Other** protocol specified also count attempts to use the Tor Browser (considered as denied access requests via the **Other** protocol).
- 

The Report Results section contains two tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) processes having allowed access. Table 2 lists the top N (where N is a specific number) processes having denied access. These tables have the following columns:

- **Process Name** - Shows a process name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

## Top active users

This report shows the most active users sorted according to the number of allowed and denied access requests sent by each user. By default, the report lists the first 10 users but you can specify any number of users.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.

- **Channel(s)** - Shows the device types and/or protocols that were selected for the report.

---

#### Note

- Reports with the **Other** protocol selected also count access requests via unidentified protocol types logged by Protocols White List rules (**Any** or **SSL** protocol) and Basic IP Firewall rules.
  - When the **Block Tor Browser traffic** security setting is in effect, reports with the **Other** protocol specified also count attempts to use the Tor Browser (considered as denied access requests via the **Other** protocol).
- 

The Report Results section contains two tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) users having allowed access. Table 2 lists the top N (where N is a specific number) users having denied access. These tables have the following columns:

- **User Name** - Shows a user name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

## Top inserted USB & FireWire devices

This report shows three groups of the most frequently inserted USB and FireWire devices sorted according to the number of the Insert actions:

- Group 1 lists both allowed and denied devices.
- Group 2 lists only allowed devices.
- Group 3 lists only denied devices.

By default, the report lists the first 10 devices in each group but you can specify any number of devices.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.

The Report Results section contains three tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) inserted USB & and FireWire devices (both allowed and denied devices). Table 2 lists the top N (where N is a specific number) inserted allowed USB & FireWire devices. Table 3 lists the top N (where N is a specific number) inserted denied USB & FireWire devices. These tables have the following columns:

- **Device Name** - Shows a device name.
- **Insert Count** - Shows the number of the Insert actions. Values in this column are sorted in descending order.

## Top used USB devices

This report shows three groups of the most frequently used USB devices sorted according to the number of access requests:

- Group 1 lists devices having both allowed and denied access.
- Group 2 lists devices having only allowed access.
- Group 3 lists devices having only denied access.

By default, the report lists the first 10 devices in each group but you can specify any number of devices.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.

The Report Results section contains three tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) USB devices having both allowed and denied access. Table 2 lists the top N (where N is a specific number) USB devices having allowed access. Table 3 lists the top N (where N is a specific number) USB devices having denied access. These tables have the following columns:

- **Device Name** - Shows a device name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

## DeviceLock Service versions

This report shows the total number of computers with the specified version(s) of DeviceLock Service and the number of computers that have different build numbers for each version.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Version(s)** - Shows the DeviceLock Service versions that were specified for the report.

The Report Results section contains a table and a pie chart that show detailed results of the report. The table has the following columns:

- **Version** - Shows a version number.
- **Build** - Shows build numbers of the version. Values in this column are sorted in descending order.
- **Number of Computers** - Shows the number of computers that have a specific build number and the total number of computers with the specified version(s) of DeviceLock Service.

The pie chart shows the percentage of computers with the specified version(s) of DeviceLock Service.

## DeviceLock Service versions by computers

This report shows the list of specified DeviceLock Service versions and computer names and the total number of computers for each version.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Version(s)** - Shows the DeviceLock Service versions that were specified for the report.

The Report Results section contains a table with detailed results of the report. This table has the following columns:

- **Version** - Shows a version number.
- **Computer name** - Shows computer names and the total number of computers for each specified version.

## DeviceLock policy changes

This report shows the list of policy change events.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header section contains the report title that appears at the very beginning of the report. The report title shows the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.

The Report Results section contains a table with detailed results of the report. This table has the following columns:

- **Date/time** - Shows the date and the time of a policy change event.
- **Action** - Shows detailed information on policy change event.
- **User** - Shows the user who modified the policy.

## Top used Printers

This report shows three groups of the most frequently used printers sorted according to the number of access requests:

- Group 1 lists printers having both allowed and denied access.
- Group 2 lists printers having only allowed access.
- Group 3 lists printers having only denied access.

By default, the report lists the first 10 printers in each group but you can specify any number of printers.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*

- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.

The Report Results section contains three tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) printers having both allowed and denied access. Table 2 lists the top N (where N is a specific number) printers having allowed access. Table 3 lists the top N (where N is a specific number) printers having denied access. These tables have the following columns:

- **Device Name** - Shows a printer name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

## Top printed documents

This report shows the most frequently printed documents (files) sorted according to the number of allowed and denied access requests:

- Group 1 lists both allowed and denied actions.
- Group 2 lists only allowed actions.
- Group 3 lists only denied actions.

By default, the report lists the first 10 documents in each group but you can specify any number of documents.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.
- **Printer(s)** - Shows the printers that were specified for the report.

The Report Results section contains three tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) documents (both allowed and denied actions). Table 2 lists the top N (where N is a specific number) documents with allowed actions. Table 3 lists the top N (where N is a specific number) documents with denied actions. These tables have the following columns:

- **File Name** - Shows a document name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

## Top copied files by extension

This report shows three groups of the most frequently copied file extensions sorted according to the number of the read and write actions:

- Group 1 lists both allowed and denied actions.
- Group 2 lists only allowed actions.
- Group 3 lists only denied actions.

By default, the report lists the first 10 file extensions in each group but you can specify any number of file extensions.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.
- **Channel(s)** - Shows the device types and/or protocols that were specified for the report.

The Report Results section contains three tables and charts with detailed results of the report. Table 1 lists the top N (where N is a specific number) file extensions (both allowed and denied actions). Table 2 lists the top N (where N is a specific number) file extensions with allowed actions. Table 3 lists the top N (where N is a specific number) file extensions with denied actions. These tables have the following columns:

- **Extension** - Shows a file extension.
- **Read** - Shows the number of read actions.
- **Write** - Shows the number of write actions.

The tables also have a **Total** row that sums up all the values in the **Read** and **Write** columns.

The **No extension** label is used for all files without an extension, and the **Other** label is used for all file extensions whose combined percentage out of the total number of files is less than 5%. The **Direct access** label is used for all CD/DVD/BD burn and direct-write operations (e.g. formatting).

## Shadow Log Reports

Shadow Log reports are based on the data held in the DeviceLock Enterprise Server shadow log files. All these reports contain the combined data from the shadow log and deleted shadow data log.

The following report types are available in this category:

- [Copied files per channel](#)
- [Top active computers](#)
- [Top active processes](#)
- [Top active users](#)
- [Top copied files](#)
- [Top copied files by extension](#)
- [Top printed documents](#)

Under each report type, the console lists the tasks that create reports of that type. For instance, the tasks for creating “Top active computers” reports of the Shadow Log category are listed in the console under **DeviceLock Enterprise Server > Reports > Shadow Log > Top active computers**. When you select a task in the console tree, the details pane lists the reports created by that task. For further details, see [Report Creation Tasks](#).

## Copied files per channel

This report shows statistics on copied files per data transmission channel (devices and/or protocols), including e-mail attachments. Statistical information on copied files is sorted according to the number of copied files and total size of all copied files separately for allowed and denied copy operations.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.
- **File Name** - Shows the files that were specified for the report.
- **Channel(s)** - Shows the data transmission channels that were specified for the report. The available options are: **all devices**, **all protocols**, and **all devices and protocols**.

The Report Results section contains four tables and four pie charts that show detailed results of the report. Table 1 shows the number of copied files for each data transmission channel for allowed copy operations. Table 2 shows the number of copied files for each data transmission channel for denied copy operations. Tables 1 and 2 have the following columns:

- **Channel** - Shows a data transmission channel.
- **Number of Files** - Shows the number of copied files.



Tables 1 and 2 also have a **Total** row that sums up all the values in the **Number of Files** column.

Table 3 shows the total size of copied files for each data transmission channel for allowed copy operations. Table 4 shows the total size of copied files for each data transmission channel for denied copy operations.

Tables 3 and 4 have the following columns:

- **Channel** - Shows a data transmission channel.
- **Data Size** - Shows the total size of all copied files.

Tables 3 and 4 also have a **Total** row that sums up all the values in the **Data Size** column.

Each table is followed by a pie chart which represents the report results in percentages.

## Top active computers

This report shows the most frequently used computers sorted according to the number of copied files and total size of all copied files. By default, the report lists the first 10 computers but you can specify any number of computers.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Channel(s)** - Shows the device types and/or protocols that were specified for the report.
- **File Name** - Shows the files that were specified for the report.

The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) computers having both allowed and denied access by the number of copied files. Table 2 lists the top N (where N is a specific number) computers having both allowed and denied access by the amount of copied data. Table 3 lists the top N (where N is a specific number) computers having allowed access by the number of copied files. Table 4 lists the top N (where N is a specific number) computers having allowed access by the amount of copied data. Table 5 lists the top N (where N is a specific number) computers having denied access by the number of copied files. Table 6 lists the top N (where N is a specific number) computers having denied access by the amount of copied data.

Tables 1, 3 and 5 have the following columns:

- **Computer Name** - Shows a computer name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

Tables 2, 4 and 6 have the following columns:

- **Computer Name** - Shows a computer name.
- **Data Size** - Shows the total size of all copied files. Values in this column are sorted in descending order.

## Top active processes

This report shows the most active processes (applications) sorted according to the number of copied files and total size of all copied files. By default, the report lists the first 10 processes but you can specify any number of processes.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Channel(s)** - Shows the device types and/or protocols that were specified for the report.
- **File Name** - Shows the files that were specified for the report.

The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) processes having both allowed and denied access by the number of copied files. Table 2 lists the top N (where N is a specific number) processes having both allowed and denied access by the amount of copied data. Table 3 lists the top N (where N is a specific number) processes having allowed access by the number of copied files. Table 4 lists the top N (where N is a specific number) processes having allowed access by the amount of copied data. Table 5 lists the top N (where N is a specific number) processes having denied access by the number of copied files. Table 6 lists the top N (where N is a specific number) processes having denied access by the amount of copied data.

Tables 1, 3 and 5 have the following columns:

- **Process Name** - Shows a process name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

Tables 2, 4 and 6 have the following columns:

- **Process Name** - Shows a process name.
- **Data Size** - Shows the total size of all copied files. Values in this column are sorted in descending order.

## Top active users

This report shows the most active users sorted according to the number of copied files and total size of all copied files. By default, the report lists the first 10 users but you can specify any number of users.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Channel(s)** - Shows the device types and/or protocols that were specified for the report.
- **File Name** - Shows the files that were specified for the report.

The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) users having both allowed and denied access by the number of copied files. Table 2 lists the top N (where N is a specific number) users having both allowed and denied access by the amount of copied data. Table 3 lists the top N (where N is a specific number) users having allowed access by the number of copied files. Table 4 lists the top N (where N is a specific number) users having allowed access by the amount of copied data. Table 5 lists the top N (where N is a specific number) users having denied access by the number of copied files. Table 6 lists the top N (where N is a specific number) users having denied access by the amount of copied data.

Tables 1, 3 and 5 have the following columns:

- **User Name** - Shows a user name.
- **Access Count** - Shows the number of access requests. Values in this column are sorted in descending order.

Tables 2, 4 and 6 have the following columns:

- **User Name** - Shows a user name.
- **Data Size** - Shows the total size of all copied files. Values in this column are sorted in descending order.

## Top copied files

This report shows the most frequently copied files, including e-mail attachments, sorted according to the number of copied files and total size of all copied files. By default, the report lists the first 10 files but you can specify any number of files.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.
- **Channel(s)** - Shows the device types and/or protocols that were specified for the report.

The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) copied files having both allowed and denied access by quantity. Table 2 lists the top N (where N is a specific number) copied files having both allowed and denied access by size. Table 3 lists the top N (where N is a specific number) copied files having allowed access by quantity. Table 4 lists the top N (where N is a specific number) copied files having allowed access by size. Table 5 lists the top N (where N is a specific number) copied files having denied access by quantity. Table 6 lists the top N (where N is a specific number) copied files having denied access by size.

Tables 1, 3 and 5 have the following columns:

- **File Name** - Shows a file name.
- **Number of Files** - Shows the number of copied files. Values in this column are sorted in descending order.

Tables 2, 4 and 6 have the following columns:

- **File Name** - Shows a file name.
- **Data Size** - Shows the total size of all copied files. Values in this column are sorted in descending order.

## Top copied files by extension

This report shows the most frequently copied file extensions sorted according to the number of copied files including e-mail attachments and total size of all copied files. By default, the report lists the first 10 file extensions but you can specify any number of file extensions.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.
- **Channel(s)** - Shows the device types and/or protocols that were specified for the report.

The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) copied file extensions having both allowed and denied access by quantity. Table 2 lists the top N (where N is a specific number) copied file extensions having both allowed and denied access by size. Table 3 lists the top N (where N is a specific number) copied file extensions having allowed access by quantity. Table 4 lists the top N (where N is a specific number) copied file extensions having allowed access by size. Table 5 lists the top N (where N is a specific number) copied file extensions having denied access by quantity. Table 6 lists the top N (where N is a specific number) copied file extensions having denied access by size.

Tables 1, 3 and 5 have the following columns:

- **Extension** - Shows a file extension.
- **Number of Files** - Shows the number of copied files. Values in this column are sorted in descending order.

Tables 1, 3 and 5 also have a **Total** row that sums up all the values in the **Number of Files** column.

Tables 2, 4 and 6 have the following columns:

- **Extension** - Shows a file extension.
- **Data Size** - Shows the total size of all copied files. Values in this column are sorted in descending order.

Tables 2, 4 and 6 also have a **Total** row that sums up all the values in the **Data Size** column.

Each table is followed by a pie chart which represents the report results in percentages.

The **No extension** label is used for all files without an extension, and the **Other** label is used for all file extensions whose combined percentage out of the total number of files is less than 5%. The **Direct access** label is used for all CD/DVD/BD burn and direct-write operations (e.g. formatting).

## Top printed documents

This report shows the most frequently printed documents (files) sorted according to the number of printed files and total size of all printed files. By default, the report lists the first 10 documents but you can specify any number of documents.

The report consists of three sections: the Report Header, Report Parameters, and Report Results.

The Report Header displays the report type.

The Report Parameters section contains information on the report parameters you specify when generating the report. This information includes:

- **Period** - Shows the start and end date and time of the log records range included in the report, according to the [Report period](#) setting in the report creation task.  
*The date/time format for the Period from: and to: fields is determined by the date/time format for the user account under which DeviceLock Enterprise Server is running.*
- **Computer(s)** - Shows the computers that were specified for the report.
- **Users(s)** - Shows the users that were specified for the report.
- **Printer(s)** - Shows the printers that were specified for the report.

The Report Results section contains six tables with detailed results of the report. Table 1 lists the top N (where N is a specific number) documents having both allowed and denied access by the number of printed files. Table 2 lists the top N (where N is a specific number) documents having both allowed and denied access by the amount of printed data. Table 3 lists the top N (where N is a specific number) documents having allowed access by the number of printed files. Table 4 lists the top N (where N is a specific number) documents having allowed access by the amount of printed data. Table 5 lists the top N (where N is a specific number) documents having denied access by the number of printed files. Table 6 lists the top N (where N is a specific number) documents having denied access by the amount of printed data.

Tables 1, 3 and 5 have the following columns:

- **File Name** - Shows a document name.
- **Number of Files** - Shows the number of printed documents. Values in this column are sorted in descending order.

Tables 2, 4 and 6 have the following columns:

- **File Name** - Shows a document name.
- **Data Size** - Shows the total size of all printed documents. Values in this column are sorted in descending order.

## Report Creation Tasks

Reports are created by tasks that can be run by hand as well as on a scheduled basis. Every run of a task creates a new report in accordance with the task settings. In the case of a scheduled run, the server creates new reports automatically as defined by the task's schedule settings.

In the DeviceLock Management Console, tasks are grouped by category and type of reports:

- Relations Chart creation tasks are listed in the **DeviceLock Enterprise Server > Reports > Relations Chart** node. To begin, select the **Create Task** command on the shortcut menu of the **Relations Chart** node. For details on this category of reports, see [Relations Charts](#).
- Report creation tasks for a particular report type of the Audit Log category are listed in the node representing that report type under **DeviceLock Enterprise Server > Reports > Audit Log** in the

console tree. To begin, select the **Create Task** command on the shortcut menu of the report type. For details on report types in this category, see [Audit Log Reports](#).

- Report creation tasks for a particular report type of the Shadow Log category are listed in the node representing that report type under **DeviceLock Enterprise Server > Reports > Shadow Log** in the console tree. To begin, select the **Create Task** command on the shortcut menu of the report type. For details on report types in this category, see [Shadow Log Reports](#).

To update the information in the task list based on the latest changes, use the **Refresh** command from the shortcut menu of the appropriate task node in the console tree or from the shortcut menu of a task in the details pane.

When you select a report creation task in the console tree, the details pane lists the task's reports. For details on the list of reports, see [Viewing Reports Created by a Task](#).

Task management involves the following activities:

- [Creating Tasks](#)
- [Managing Existing Tasks](#)
- [Viewing Reports Created by a Task](#)

---

#### Note

When multiple instances of DeviceLock Enterprise Server use the same database, the tasks and reports created on one of them can be viewed and administered on any one of those server instances. The task is executed by the server where it was created or changed the last time.

---

## Creating Tasks

Creating a task requires the following steps:

1. Decide on the report category and type for which to create the task.  
The task can generate either [Relations Charts](#) or a certain type of [Audit Log Reports](#) or [Shadow Log Reports](#).
2. Execute the **Create Task** command for the appropriate category and report type:
  - If a task is required to generate Relations Charts, choose the command from the shortcut menu of the **DeviceLock Enterprise Server > Reports > Relations Chart** node.
  - If a task is required to generate Audit Log reports of a certain type, choose the command from the node representing that report type under **DeviceLock Enterprise Server > Reports > Audit Log** in the console tree.
  - If a task is required to generate Shadow Log reports of a certain type, choose the command from the node representing that report type under **DeviceLock Enterprise Server > Reports > Shadow Log** in the console tree.
3. Configure report options in the dialog box that appears (see [Dialog box for configuring report options](#)) and then click **Next** to proceed to configuring task schedule and other options.
4. Configure task schedule and other options in the dialog box that appears (See [Dialog box for configuring task schedule and options](#)) and then click **Finish** to complete.

## Dialog box for configuring report options

This dialog box serves to view or change report options. It is the first displayed when configuring a report creation task. The options it provides depend upon the category and type of reports that the task creates. This section describes all the possible report options. In the description of each option, it is indicated to which reports the option is applicable.

All possible report options are as follows:

- Report period
- Contact(s)
- Include internal user(s)
- Exclude internal user(s)
- Exclude external contact(s)
- Computer(s)
- Version(s)
- User(s)
- File name
- Printer(s)
- Threshold
- Report Devices
- Report TS Devices as regular devices
- Report Protocols
- Access type(s)
- Device type(s)
- Protocol(s)
- Top computers
- Top Printers
- Top users
- Top USB and FireWire devices
- Top USB devices
- Top processes
- Top files
- Top printed documents

### Report period

The following options specify the date range of log records to include in the report:

- **From** - You can choose the range beginning from the earliest record date in the log (option **First Record**), or select a certain date (option **Records On**). In the latter case, the report includes only data from the records made no earlier than the selected date.



- **To** - Together with the **From** setting, you can set the range end to the latest record date in the log (option **Last Record**), or select a certain date (option **Records On**). In the latter case, the report includes only data from the records made no later than the selected date.
- **Last** - If you select this option instead of **From**, you can configure the report to include only data from the records for a certain number of past days, weeks, or months before the date that the report is generated. Select the desired number and time unit (days, weeks, or months).

## Contact(s)

This option specifies a list of contacts to include in the report. It is available only for Relations Charts.

A contact is an e-mail address, a social network user ID or an instant messenger user ID, etc. Contacts can be used to identify users who have an account in the organization's domain (internal users) as well as users without such an account (external contacts).

When created with this option, the Relations Chart shows the specified contacts along with the users who communicated with those contacts. Using such a Relations Chart, it is easy to find out who exchanges files and messages with certain persons outside or inside the organization:

- The Relations Chart displays only users who communicated with at least one of the specified contacts, as well as objects related to such users. Other users and their related objects are hidden.
- On the Relations Chart, the specified contacts are highlighted in green, and are circled by default.
- For each of the specified contacts, the Relations Chart by default reveals and expands the following objects:
  - In the case of an external contact - objects related to the user who most actively communicated with that contact.
  - In the case of a contact that belongs to an internal user - objects related to that user.

In this way, Relations Charts help locate specific contacts and identify their relationships with users.

To specify the contacts to be shown in the report, do one of the following:

- In the **Contact(s)** box, type contact names or IDs, separating them with a semicolon (;). In a contact name or ID, you could use wildcards: an asterisk (\*) to represent any sequence of characters, a question mark (?) to represent any single character.  
- OR -
- Click **Load** to import contacts from a text file that specifies each contact's name or ID on a separate line.

## Include internal user(s)

This option specifies a list of internal users to include in the report. It is available only for Relations Charts.

Internal users are inside the corporate network and are members of your organization's domain.

To specify internal users for the report, select any of the following options:

- **All** - This option is selected by default. If you select this option, the report will display data for all users in the DeviceLock logs.
- **Static list** - This option lets you specify a static list of users that will never change. If you select this option:
  1. Click **Edit** to open the **Edit static list** dialog box.
  2. In the **Edit static list** dialog box, select users by using one of the following options: **Active Directory**, **LDAP**, **From File**, **Manual**, and then use the **>**, **>>**, **<**, **<<** buttons to add selected users to the **Selected user(s)** list or remove users from that list.  
 The **Active Directory** option lets you select users from Active Directory. You can click the **...** button to specify the user name and password for access to Active Directory.  
 The **LDAP** option lets select users from an LDAP directory. Click the **...** button to specify the connection parameters for access to the directory.  
 The **From File** option lets you import a list of users from a text file and then select users. To open such a file, click the **...** button. A text file must contain each user's name on a separate line and can be either Unicode or non-Unicode.  
 The **Manual** option lets you specify users by typing user names. Each user's name must be typed on a separate line. You can also click the **...** button to select users by using the **Select Users or Groups** dialog box.  
*The selected users are displayed under Selected user(s) in the right pane of the dialog box.*  
*To remove single users from the list of selected users, use the left single-arrow button **<**. To add or remove all available users to or from the list of the selected users at the same time, use the right double-arrow button **>>** or left double-arrow button **<<**.*  
*You can use wildcards such as asterisks (\*) and question marks (?). An asterisk (\*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity.*
- **Dynamic list** - This option lets you specify a dynamic list of users that will update every time the report is created, adding or removing users from the list as they are added or removed from the selected container in the directory. If you choose this option:
  1. Click **Edit** to open the **Edit dynamic list** dialog box.
  2. In the **Edit dynamic list** dialog box, browse the AD or LDAP tree to find the required container, and then click **Select**. You can select one or more containers. To include users located in lower-level containers within the one you selected, select the **Traverse subcontainers when enumerating users** check box. To perform Active Directory synchronization, select the **Synchronization** check box.  
 By clicking the **...** button you can specify the user name and password for access to AD (if the **Active Directory** option is selected) or connection parameters for access to the LDAP server (if the **LDAP** option is selected).

## Exclude internal user(s)

This option specifies a list of internal users to be excluded from the report. It is available only for Relations Charts.

Internal users are inside the corporate network and are members of your organization's domain.

To specify internal users that are to be excluded from the report, do one of the following:

- In the **Exclude internal user(s)** box, type user names. You can use wildcards, such as asterisks (\*) and question marks (?). Specify a user name using the following format: <DomainName>\<UserName>. The default value in this box is NT Authority\\*, which excludes the internal Windows accounts, such as Local Service, Network Service and Local System, from the report.  
*An asterisk (\*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity. Multiple user names must be separated by a semicolon (;).*  
- OR -
- Click **Browse** to open and use the **Select Users** dialog box. In the **Select Users** dialog box, do the following:
  - **Object Types** - Select the desired object types.
  - **Locations** - Select the folder to search for objects.
  - **Enter the object names to select** - Type the object names to find and select. Multiple object names must be separated by a semicolon (;).
  - **Check Names** - Click to find object names that match those entered in the **Enter the object names to select** box.
  - **Advanced** - Click to perform an advanced search for objects.- OR -
- Click **Load** to import a list of users from a text file that specifies each user's name on a separate line in the following format: <DomainName>\<UserName>.

## Exclude external contact(s)

This option specifies a list of external contacts to be excluded from the report. It is available only for Relations Charts.

External contacts are e-mail addresses, social network and instant messenger IDs of users who are outside the corporate network and are not members of your organization's domain.

To specify external contacts that are to be excluded from the report, do one of the following:










- In the **Exclude external contact(s)** box, type contact names or IDs, separating them with a semicolon (;).  
In a contact name or ID, you could use wildcards: an asterisk (\*) to represent any sequence of characters, a question mark (?) to represent any single character.  
- OR -
- Click **Load** to import contacts from a text file that specifies each contact's name or ID on a separate line.



## Computer(s)

This option specifies computers for the report. It is available for all reports except “Top active computers” and Relations Charts.


The **Computer(s)** box is empty by default. This means that the report will include data for all computers in the DeviceLock Enterprise Server database.

To specify computers for the report, you can do any of the following:




- In the **Computer(s)** box, type computer names using wildcards, such as asterisks (\*) and question marks (?). For example, if you specify \*.mydomain.com, the report will display data for all computers in the domain mydomain.com.  
*An asterisk (\*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity. Multiple computer names must be separated by a comma (,) or semicolon (;).*  
- OR -
- Click **Browse** next to the **Computer(s)** box, and then use one of the following options in the **Edit computers list** dialog box that appears:
  - **Active Directory** - This option is selected by default. This option lets you select computers from Active Directory. If you select this option:
    - a. Click the  button to supply alternative credentials to access Active Directory. For more information, see [description of Active Directory credentials](#).
    - b. In the left pane of the **Edit computers list** dialog box, select the appropriate check boxes next to desired computers.
    - c. Click the right single-arrow button .  
*The selected computers are displayed under Selected computers in the right pane of the dialog box.*  
*To remove single computers from the list of selected computers, use the left single-arrow button .*  
*To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button  or left double-arrow button .*
- **From Database** - This option lets you select computers from the DeviceLock Enterprise Server database that shows all computers from which the server has ever received audit and shadow data. If you select this option:
  - a. In the left pane of the **Edit computers list** dialog box, select the appropriate check boxes next to desired computers.
  - b. Click the right single-arrow button .  
*The selected computers are displayed under Selected computers in the right pane of the dialog box.*  
*To remove single computers from the list of selected computers, use the left single-arrow button .*  
.  
*To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button  or left double-arrow button .*


- **LDAP** - This option lets you select computers from an LDAP-compatible directory service. If you select this option:
  - a. Click the  button to open the **LDAP Settings** dialog box and configure a connection to the LDAP server. For more information, see the [description of LDAP settings](#).
  - b. In the left pane of the **Edit computers list** dialog box, select the appropriate check boxes next to desired computers.
  - c. Click the right single-arrow button .
 

*The selected computers are displayed under Selected computers in the right pane of the dialog box.*


*To remove single computers from the list of selected computers, use the left single-arrow button .*

.




*To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button  or left double-arrow button .*
- **From File** - This option lets you select computers from an external text file. A text file must contain each computer's name or IP address on a separate line and can be either Unicode or non-Unicode. If you select this option:
  - a. Click the  button to open the **Open** dialog box and browse for the file to use.
  - b. In the **Open** dialog box, in the **Look in** list, click the location that contains the file you want to import.
  - c. In the folder list, locate and open the folder that contains the file.
  - d. Click the file, and then click **Open**.
 

*The computers from the file are displayed in the left pane of the Edit computers list dialog box.*
  - e. In the left pane of the **Edit computers list** dialog box, select the desired computers, and then click the right single-arrow button .
 


*The selected computers are displayed under Selected computers in the right pane of the dialog box.*

*To remove single computers from the list of selected computers, use the left single-arrow button .*



.

*To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button  or left double-arrow button .*
- **Manual** - This option lets you manually add computers that you want to select for the report. If you select this option:
  - a. In the left pane of the **Edit computers list** dialog box, type either computer names or IP addresses. Press the ENTER key after each computer name to make sure that each computer name is on a separate line.
  - b. In the left pane of the **Edit computers list** dialog box, select the desired computers, and then click the right single-arrow button .
 

*The selected computers are displayed under Selected computers in the right pane of the dialog box.*

*To remove single computers from the list of selected computers, use the left single-arrow button .*

.

*To add or remove all available computers to or from the list of selected computers at the same time, use the right double-arrow button  or left double-arrow button .*

## Version(s)

This option specifies DeviceLock Service versions for the report. It is available only for “DeviceLock Service versions” and “DeviceLock Service versions by computers” reports.

The **Version(s)** box is empty by default. This means that the report will display data for computers with all versions of DeviceLock Service in the DeviceLock Enterprise Server database.

To specify versions for the report, in the **Version(s)** box, type version numbers using wildcards, such as asterisks (\*) and question marks (?). For example, type 6.4.? to specify version 6.4.x.

*An asterisk (\*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity. Multiple versions must be separated by a comma (,) or semicolon (;).*

## User(s)

This option specifies users for the report. It is available for all reports except “Top active computers”, “Top active users”, “Top active processes” and Relations Charts.

The **User(s)** box is empty by default. This means that the report will display data for all users in the DeviceLock Enterprise Server database.

To specify users for the report, do one of the following:

- In the **User(s)** box, specify user names using wildcards, such as asterisks (\*) and question marks (?). For example, if you specify mydomain\*, the report will display data for all users in mydomain.  
*An asterisk (\*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity. Multiple user names must be separated by a comma (,) or semicolon (;).*

---

### Note

You cannot specify user groups in the **User(s)** box.

---

- OR -

- Click **Browse** next to the **User(s)** box, and then do the following:
  - a. In the **Select Users** dialog box that opens, in the **Enter the object names to select** box, type the user account names that you want to specify for the report.  
*Multiple user names must be separated by a semicolon (;).*
  - b. Click **OK**.

## File name

This option specifies files for the report. It is available only for “Top active users”, “Top active computers”, “Top active processes” and “Copied files per channel” reports of the Shadow Log category.

The **File name** box is empty by default. This means that the report will display data for all files in the DeviceLock Enterprise Server database.

To specify files for the report, in the **File name** box, type file names using wildcards, such as asterisks (\*) and question marks (?). For example, type \*.txt to specify all files with the .txt file name extension. To continue the example, if you want to specify all files whose names begin with any characters that contain the string "price" and have any extension, type \*price\*.\*

*An asterisk (\*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity. Multiple file names must be separated by a comma (,) or semicolon (;).*

## Printer(s)

This option specifies printer names for the report. It is available only for "Top printed documents" reports.

The **Printer(s)** box is empty by default. This means that the report will display data for all printers available in the DeviceLock Enterprise Server database.

To specify printer names for the report, in the **Printer(s)** box, type names using wildcards, such as asterisks (\*) and question marks (?). For example, type PDF\* to specify all printers whose names begin with PDF.

*An asterisk (\*) replaces an unlimited number of characters. The question mark (?) replaces a single character. You can use these wildcards in any position and in any quantity. Multiple names must be separated by a comma (,) or semicolon (;).*

## Threshold

This option specifies the time interval, in seconds, between logged events, and is used for event consolidation. It is available for all reports of the Audit Log report category except "Top inserted USB & FireWire devices" reports.

Given that a single user action often causes multiple events, DeviceLock consolidates events when retrieving them from the audit log for reporting purposes. DeviceLock compares the time stamp of the event with the time stamp of subsequent events. When this time delta is less than or equal to the **Threshold** value, multiple events of the same type (either Allowed or Denied) are combined into a single summary event if all of the following conditions are true:

- The events are associated with the same computer.
- The events are associated with the same device type or protocol.

## Report Devices

Select the **Report Devices** check box if you want the report to include data for all device types. If you do not select this check box, information on all device-related activities will be excluded from the report. This check box is available only for "Allowed & Denied access requests per channel", "Allowed vs. Denied access requests", and "Copied files per channel" reports.

## Report TS Devices as regular devices

Select the **Report TS Devices as regular devices** check box if you want the report to count TS Devices data together with regular devices data:

- TS Devices (Mapped drives) -> Removable
- TS Devices (Serial port) -> Serial port
- TS Devices (USB devices) -> USB Devices
- TS Devices (Clipboard) -> Clipboard

If you do not select this check box, the data specific to TS Devices will be counted and displayed separately. This check box is available only for "Allowed & Denied access requests per channel", "Read & Write access requests per device type" and "Copied files per channel" reports.

## Report Protocols

Select the **Report Protocols** check box if you want the report to include data for all protocols. If you do not select this check box, information on all protocol-related activities will be excluded from the report. This check box is available only for "Allowed & Denied access requests per channel", "Allowed vs. Denied access requests" and "Copied files per channel" reports.

## Access type(s)

This option specifies the types of events to be included in the report. It is available only for "Read & Write access requests per device type" reports of the Audit Log category.

If you select the **Allowed** check box, the Success Audit events (that is, events that record successful access attempts) will be included in the report. If you select the **Denied** check box, the Failure Audit events (that is, events that record failed access attempts) will be included in the report. You can use either or both of these options to specify the types of events.

## Device type(s)

This option specifies the device types to be included in the report. It is available only for "Top active computers", "Top active users", "Top copied files", "Top active processes" and "Top copied files by extension" reports.

If you choose this option, select check boxes next to the device types you want to include in the report.

## Protocol(s)

This option specifies the protocols to be included in the report. It is available for Relations Charts as well as for "Top active computers", "Top active users", "Top copied files", "Top active processes" and "Top copied files by extension" reports.

If you choose this option, select check boxes next to the protocols you want to include in the report.



---

## Note

- If you leave both options - **Device type(s)** and **Protocol(s)** - unselected, the report will display data for all device types and protocols. If you select either of these options and then specify device type(s) or protocols, the report will display data only for the specified device type(s) or protocols.
  - The **Other** protocol, which represents data transmitted via unrecognized protocols logged by Protocols White List (**Any** and **SSL**) and Basic IP Firewall rules, can also be selected.
  - When the **Other** protocol is selected and the **Block Tor Browser traffic** security setting is in effect, the report also accounts for the number of attempts to use the Tor Browser (considered as denied access requests via the **Other** protocol).
- 

## Top computers

This option specifies the number of the most frequently used computers to include in the report. It is available only for “Top active computers” reports.

The default value is 10. To change the default value, enter the desired number of computers in the **Top computers** box.

## Top Printers

This option specifies the number of the most frequently used printers to include in the report. It is available only for “Top used Printers” reports.

The default value is 10. To change the default value, enter the desired number of printers in the **Top Printers** box.

## Top users

This option specifies the number of the most active users to include in the report. It is available only for “Top active users” reports.

The default value is 10. To change the default value, enter the desired number of users in the **Top users** box.

## Top USB and FireWire devices

This option specifies the number of the most frequently inserted USB and FireWire devices to include in the report. It is available only for “Top inserted USB & FireWire devices” reports.

The default value is 10. To change the default value, enter the desired number of devices in the **Top USB and FireWire devices** box.

## Top USB devices

This option specifies the number of the most frequently used USB devices to include in the report. It is available only for “Top used USB devices” reports.

The default value is 10. To change the default value, enter the desired number of devices in the **Top USB devices** box.

### Top processes

This option specifies the number of the most active processes to include in the report. It is available only for “Top active processes” reports.

The default value is 10. To change the default value, enter the desired number of processes in the **Top processes** box.

### Top files

This option specifies the number of the most frequently copied files to include in the report. It is available only for “Top copied files” and “Top copied files by extension” reports.

The default value is 10. To change the default value, enter the desired number of files in the **Top files** box.

### Top printed documents

This option specifies the number of the most frequently printed documents to include in the report. It is available only for “Top printed documents” reports.

The default value is 10. To change the default value, enter the desired number of documents in the **Top printed documents** box.

## Dialog box for configuring task schedule and options

This dialog box is displayed second in the series of dialog boxes for configuring report creation tasks. Having configured report options, this dialog box can be used to view or change the task’s schedule and other options, including:

- **Task name** - The name of the task cannot be blank or consist solely of spaces. Each task must have a unique name on the server.
- **Active** - If this check box is selected, the task runs automatically by the schedule specified.
- **Schedule** - The following options are used to configure a schedule:
  - **One Time** - Choose the date and time to run the task, or select the **Now** check box to run the task right after it has been created or modified. The task will run only one time.
  - **Hourly** - Choose the recurrence interval for the task and the date and time to run the task. For example, an interval of 1 produces an hourly schedule and an interval of 2 produces an every-other-hour schedule. The task will run each hour.
  - **Daily** - Choose the recurrence interval for the task and the date and time to run the task. For example, an interval of 1 produces a daily schedule and an interval of 2 produces an every-other-day schedule. The task will run at the specified time each day.
  - **Weekly** - Choose the recurrence interval for the task, the date and time to run the task, and the days of the week on which to run the task. For example, an interval of 1 produces a weekly

schedule and an interval of 2 produces an every-other-week schedule. The task will run at the specified time on each of the specified days.

- **Monthly** - Choose the months in which to run the task and the weeks of the month and the days of the week for each month in which to run the task. The task can also be configured to run on a certain last day of each month.
- **Send report via e-mail** - To deliver the task's reports via e-mail, select this check box and complete the following fields:
  - **Recipients** - Specify the e-mail addresses of the report recipients. You can specify multiple addresses separated by a semicolon (;).
  - **Report format** - Select the format in which to send this task's reports. The default format is initially selected (see [Setting Default Format for Reports](#)).

---

#### Note

- Options for sending reports are not displayed when configuring a Relations Chart creation task as Relations Charts cannot be sent by e-mail.
  - To send reports, a mail server must be specified (see [Configuring E-mail Delivery of Reports](#)). Otherwise, the options for sending reports are not available.
- 

## Managing Existing Tasks

When the **Relations Chart** node or a report type is selected in the console tree, the details pane lists report creation tasks, with the following information on each task:

- **Name** - The name of the task.
- **Status** - One of the following:
  - **Waiting** - Task is waiting for a subsequent run on a schedule.
  - **Running** - Task is in progress.
  - **Finished** - Last execution of the task successfully completed.
  - **Error** - Task encountered an error.
- **Schedule** - Identifies the task schedule.
- **Last Run Time** - Date and time of the last run of this task.

The shortcut menu on a task provides the following commands:

- **Edit Task** - Opens the dialog boxes to view or change the settings of the selected task.
- **Duplicate Task** - Creates a new task with the settings copied from the selected task. The settings of the new task can be edited in the dialog boxes that appear.
- **Delete Task/Delete Tasks** - Deletes the selected task or tasks. Multiple tasks can be selected by using the Shift or Ctrl key. Deleting a task also deletes all its reports.
- **Run Task/Run Tasks** - Allows you to start the selected task or tasks by hand regardless of the schedule.
- **Stop Task** - Allows you to stop running the task that was started by hand.
- **Refresh** - Updates the list with the most recent information.

The commands on the shortcut menu can be used to:

- **Run a task** - Click **Run Task**. Running a task results in generating a new report. The **Run Tasks** command can be used to run multiple selected tasks at a time.
- **View or change the report options for a task** - Click **Edit Task**, and then view or change the options in the dialog box that appears (see [Dialog box for configuring report options](#)). When done, click **Next**, and then click **Finish**.

- **View or change the name, schedule, or other options for a task** - Right-click the task, click **Edit Task**, click **Next**, and then view or change the options in the dialog box that appears (see [Dialog box for configuring task schedule and options](#)). When done, click **Finish**.

The dialog boxes for editing tasks are almost the same as those for creating tasks. The only difference is that the dialog boxes for editing display the current settings, and allow you to make and apply your changes to the selected task instead of creating a new one.

- **Create a new task by copying an existing one** - Right-click the task to copy, click **Duplicate Task**, and then use the dialog boxes displayed by that command to view or change the settings for the new task (see [Dialog box for configuring report options](#), [Dialog box for configuring task schedule and options](#)).

The dialog boxes for duplicating tasks are almost the same as those for creating tasks. The only difference is that the dialog boxes for duplicating are pre-populated with the settings copied from the selected task.

- **Delete some tasks** - Select one or more tasks, right-click the selection, and then click **Delete Task** (in the case of a single task) or **Delete Tasks** (in the case of multiple tasks). To select multiple tasks, use the Shift or Ctrl key. A task can be deleted even if it has any reports. In this case, the console prompts for confirmation and then deletes the task along with all its reports if the console user has confirmed their deletion.

## Viewing Reports Created by a Task

When a task is selected in the console tree, the details pane lists the reports created by that task, with the following information on each report:

- **Name** - By default, the name of the report is composed of the task name followed by the date and time the task was started.
- **Type** - Can be **Scheduled** or **Manual**, depending on whether the task was run by a schedule or by hand, respectively.
- **Status** - One of the following:
  - **Generating** - Report creation is in progress.
  - **Ready** - Report created successfully.
  - **Error** - Report encountered an error. Click this status to view the error message. Use [Server Log Viewer](#) to find more information about the error.
- **E-mailed** - Appears only for Audit Log reports and Shadow Log reports. Possible values:
  - **Yes** - The report included in the e-mail delivery was successfully delivered to some or all of the intended recipients. **Yes** is displayed only after the sending process is complete.

- **No** - Indicates one of the following:
  - The report is not included in the e-mail delivery.
  - OR -
  - The report included in the e-mail delivery did not reach all of the intended recipients.

If an error occurs during the e-mail delivery of a report, you can use [Server Log Viewer](#) to determine the reason.

*If your computer has anti-virus or anti-spam software installed and running and an error occurs during the e-mail delivery of a report, the error information may not be reported in the DeviceLock Enterprise Server log. This behavior occurs because anti-virus and anti-spam products, for example, Symantec Norton AntiVirus, can automatically intercept e-mail traffic.*

*For information about how your anti-virus or anti-spam program works, consult the manufacturer's documentation included with your program.*

- **Started** - Date and time that the report creation started.
- **Finished** - Date and time that the report creation was completed.
- **Scheduled by** - Identifies the user account that started the task of creating this report.
- **Scheduled from** - Identifies the computer from which the report creation task was started.

The shortcut menu on a report in the details pane provides the following commands:

- **Open** - Displays the report.
- **Rename** - Changes the name of the selected report.
- **Send via e-mail** - Sends the completed report through e-mail. Enter the report recipient addresses in the dialog box that appears when you select this command. This command is not available in the menu for Relations Charts.
- **Save As** - Exports the report to a file. Hover over this command to select the export format. This command is not available in the menu for Relations Charts.
- **View parameters** - Opens the dialog box to view the report options of that report.
- **Delete Report/Delete Reports** - Deletes the selected report or reports. Multiple reports can be selected by using the Shift or Ctrl key.
- **Refresh** - Updates the list of reports with the most recent information.

---

#### Note

- There are no commands **Send via e-mail** and **Save As** in the menu for the Relations Chart as Relations Charts cannot be sent by e-mail or saved as files.
  - The **Send via e-mail** command requires a mail server to be specified (see [Configuring E-mail Delivery of Reports](#)). Otherwise, this command does not appear on the menu.
- 

For details on report management activities, see [Working with Reports](#).

# Configuring E-mail Delivery of Reports

DeviceLock can send reports by e-mail using an SMTP server. To enable e-mail delivery of reports, you must specify the SMTP server through which reports will be sent as well as recipient addresses to which reports will be delivered.

---

## Note

Relations Charts and User Dossiers cannot be sent by e-mail.

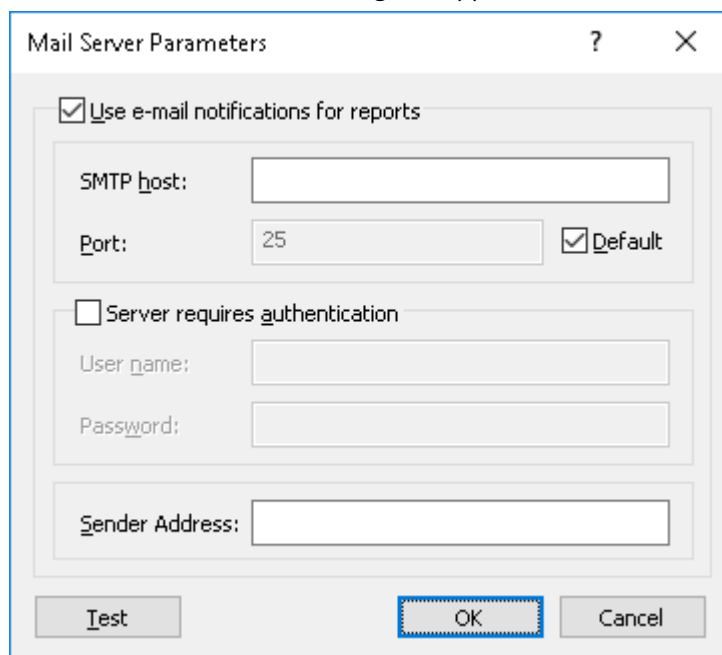
---

### To configure e-mail delivery of reports

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, right-click **Reports**, and then click **Notification Settings**.  
- OR -

Select **Reports**, and then click **Notification Settings**  on the toolbar.

The Mail Server Parameter dialog box appears.



The image shows the 'Mail Server Parameters' dialog box. It has a title bar with a question mark and a close button. The main area contains several fields and checkboxes. At the top, there is a checked checkbox labeled 'Use e-mail notifications for reports'. Below this, there are three input fields: 'SMTP host:', 'Port:', and 'Sender Address:'. The 'Port:' field has the value '25' and a checked checkbox labeled 'Default'. Below the 'SMTP host:' field, there is an unchecked checkbox labeled 'Server requires authentication'. Below this checkbox, there are two input fields: 'User name:' and 'Password:'. At the bottom of the dialog, there are three buttons: 'Test', 'OK', and 'Cancel'. The 'OK' button is highlighted with a blue dashed border.

4. In the **Mail Server Parameter** dialog box, do the following:
  - **Use e-mail notifications for reports** - To enable the delivery of reports by e-mail, select this check box and enter e-mail server (SMTP) settings in the respective fields of the dialog box. Clear the **Use e-mail notifications for reports** check box if you want to disable the delivery of reports by e-mail.
  - **SMTP host** - Specify the SMTP server to send reports. In this field, enter the name or IP address of the server.

- **Port** - Specify the port for connecting to the SMTP server. The default port is 25. Clear the **Default** check box if you want to enter a different port number.

---

**Note**

DeviceLock supports both unencrypted and SSL-encrypted connections to the SMTP server. The connection type is set automatically, depending upon whether SSL is enabled on the SMTP server.

---

- **Server requires authentication** - Select this check box if authentication is required to connect to the SMTP server you have specified. Otherwise, leave this check box cleared. If the **Server requires authentication** check box is selected, the **User name** and **Password** fields must specify the name and password of an e-mail account that has permission to connect to the SMTP server.
  - **Sender Address** - Supply the address to display in the **From** field of the e-mail messages with DeviceLock reports.
5. Optionally, click **Test** to verify the mail server settings.
  6. In the dialog box that appears when you click **Test**, specify the address of the mail recipient, and click **OK** to send a test message via the mail server specified.  
In case of valid mail server settings, the message is delivered to the recipient. Otherwise, the console displays an error message describing the problem.
  7. When finished, click to **OK**.

## Setting Default Format for Reports

You can specify the report output format you want to use for reports. The available options are:

- HTML Format (\*.htm)
- PDF Format (\*.pdf)
- Rich Text Format (\*.rtf)

DeviceLock uses PDF as the default output format for reports.

### *To set the default format for reports*

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, expand **DeviceLock Enterprise Server**.
3. Under **DeviceLock Enterprise Server**, right-click **Reports**, point to **Set Default Format**, and then click any of the following options: **HTML**, **PDF**, **RTF**.

---

**Note**

Setting format for reports has no effect on Relations Charts and User Dossiers.

---

## Working with Reports

This section provides summary instructions on how to perform the following operations:

- [Generating Reports](#)
- [Refreshing Lists of Reports](#)
- [Viewing Reports](#)
- [Viewing Report Parameters](#)
- [Exporting and Saving Reports](#)
- [Sending Reports by E-mail](#)
- [Deleting Reports](#)

---

### Important

These instructions do not apply to [User Dossiers](#).

---

## Generating Reports

Reports are generated by tasks that can be run on a schedule as well as by hand. Every run of a task generates a new report. For further details, see [Report Creation Tasks](#).

### *To generate a report*

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, under **DeviceLock Enterprise Server > Reports**, locate the task for generating the desired report.  
Create the task if it does not exist. For instructions, see [Creating Tasks](#).
3. Do one of the following:
  - To generate the report right away, right-click the task and click **Run Task**.
  - To generate the report on a schedule, right-click the task, click **Edit Task**, and proceed to the dialog box for configuring the schedule. View or change the task's schedule there (see [Dialog box for configuring task schedule and options](#)).

To view report creation results, select the task in the console tree. Information about reports is displayed in the details pane (see [Viewing Reports Created by a Task](#)).



## Refreshing Lists of Reports

When you select a task in the console tree, the details pane lists the reports created by that task. Since the console does not update the list automatically, the refreshing of the list must be performed by hand.

### *To refresh the list of reports*

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, under **DeviceLock Enterprise Server > Reports**, locate the task that creates the desired reports.



3. Do one of the following:
  - Right-click the task and click **Refresh**, or select the task and click **Refresh**  on the toolbar.
  - Right-click any report in the list and click **Refresh**, or select a report in the list and click **Refresh**  on the toolbar.

## Viewing Reports

Once a report has been successfully created, you can open and view it in DeviceLock Management Console.

### *To view a report*

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, under **DeviceLock Enterprise Server > Reports**, locate and select the task that created the desired report.
3. In the list of reports that appears in the details pane, right-click the report and click **Open**.

To view a Relations Chart, you can also select it under the corresponding task in the console tree.

Audit/Shadow Log reports open in the application associated with the default format selected for reports. Normally, this is Adobe Acrobat Reader since PDF is initially selected as the default format. Acrobat Reader can be installed from the Adobe website at [get.adobe.com/reader](http://get.adobe.com/reader).

## Viewing Report Parameters

Every report generated and stored on the server holds information about the report parameters that were set when generating that report. You can view them in DeviceLock Management Console.

### *To view report parameters*

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, under **DeviceLock Enterprise Server > Reports**, locate and select the task that created the desired report.
3. In the list of reports that appears in the details pane, right-click the report and click **View parameters**.

Parameter values are displayed in the dialog box that appears, similar to the one used when creating a task (see [Dialog box for configuring report options](#)).

## Exporting and Saving Reports

Reports generated and stored on the server can be exported to files of different formats (HTML, PDF or RTF), to be saved locally or on the network.

---

### Important

Relations Charts cannot be exported and saved to files as these are interactive reports.

---

#### *To export and save a report*

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, under **DeviceLock Enterprise Server > Reports > Audit Log** or **DeviceLock Enterprise Server > Reports > Shadow Log**, locate and select the task that created the desired report.
3. In the list of reports that appears in the details pane, right-click the report, point to **Save As**, and click the desired export format: HTML, PDF or RTF.
4. In the dialog box that appears, choose the folder and specify the name of the file to hold the exported report. The default name of the file is composed of the report name followed by the current date and time.

It is possible to export and save multiple reports at a time:

1. In the list of reports, click while holding down the Shift or Ctrl key to select reports.
2. Right-click the selection, point to **Save As**, and click the export format to use.
3. In the dialog box that appears, choose the folder to hold the files with the exported reports.

---

### Note

Reports exported in HTML format are saved as .htm files. If the original report contains any graphic images, each image is saved as a separate .gif file in the folder containing the .htm file.

---

## Sending Reports by E-mail

DeviceLock provides the following options to send reports by e-mail:

- Every task for creating reports provides the option to send results via e-mail (see [Dialog box for configuring task schedule and options](#)). Having this option enabled, the task sends every newly-created report to the specified e-mail recipients.
- The console provides a command to send completed reports to the specified e-mail recipients.

Mail server must be specified to send reports by e-mail. For details on mail server, see [Configuring E-mail Delivery of Reports](#).

---

### Important

Relations Charts cannot be sent by e-mail as these are interactive reports.

---

#### *To send a completed report by e-mail*

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.

2. In the console tree, under **DeviceLock Enterprise Server > Reports > Audit Log** or **DeviceLock Enterprise Server > Reports > Shadow Log**, locate and select the task that created the desired report.
3. In the list of reports that appears in the details pane, right-click the report and click **Send via e-mail**.
4. In the dialog box that appears, type the addresses of the e-mail recipients in the following format: user@mailserver. Separate addresses by a comma, semicolon, or space.

It is possible to send multiple reports at a time:

1. In the list of reports, click while holding down the Shift or Ctrl key to select reports.
2. Right-click the selection and click **Send via e-mail**.
3. In the dialog box that appears, type the addresses of the desired e-mail recipients.

If an error occurs upon the delivery of the report, an error message is recorded in the server log. To view error messages, use [Server Log Viewer](#).

---

**Note**

Reports in HTML are sent in the message body rather than as attachments.

---

## Deleting Reports

DeviceLock Management Console provides the option to delete reports from the server.

### ***To delete a report***

1. Open DeviceLock Management Console and connect it to the computer running DeviceLock Enterprise Server.
2. In the console tree, under **DeviceLock Enterprise Server > Reports**, locate and select the task that created the desired report.
3. In the list of reports that appears in the details pane, right-click the report and click **Delete Report**.

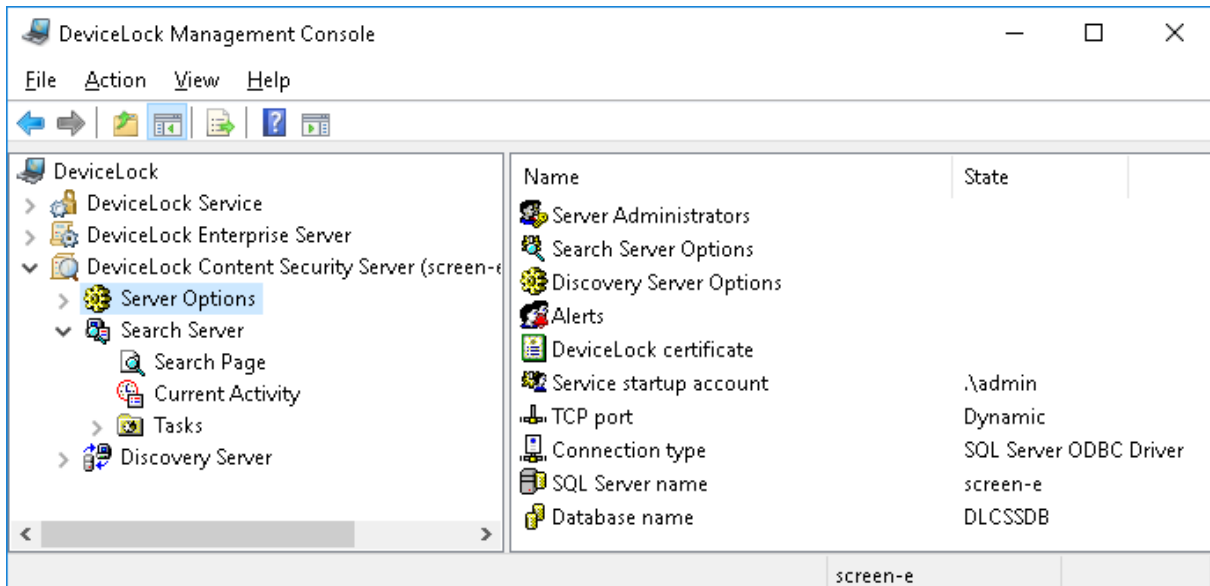
It is possible to delete multiple reports at a time:

1. In the list of reports, click while holding down the Shift or Ctrl key to select reports.
2. Right-click the selection and click **Delete Reports**.

# DeviceLock Content Security Server

## Administering DeviceLock Content Security Server

Use the **DeviceLock Content Security Server** node in the DeviceLock Management Console to configure and use the DeviceLock Content Security Server.



Right-click the **DeviceLock Content Security Server** node to display the following commands:

- **Connect** - Connects to the computer running the DeviceLock Content Security Server. For more information, see [Connecting to Computers](#).  
When connecting to a computer where an old version of the DeviceLock Content Security Server is installed, the following message may appear: "The product version on the client and server machines does not match." In this case, install the new version of the DeviceLock Content Security Server on this computer. For installation instructions, see [Installing DeviceLock Content Security Server](#).
- **Reconnect** - Connects to the currently connected computer once again.
- **Connect to Last Used Server at Startup** - Click this command to instruct the DeviceLock Management Console to automatically connect to the last used server each time the console starts up.
- **Certificate Generation Tool** - Starts a tool for generating DeviceLock certificates. See [Generating DeviceLock Certificates](#) for details.
- **DeviceLock Signing Tool** - Starts a tool to grant users temporary access to requested devices and to sign DeviceLock Service settings files. See [DeviceLock Signing Tool](#) for details.
- **About DeviceLock** - Displays a dialog box with information about the DeviceLock version and licenses.

Expand the **DeviceLock Content Security Server** node to display the following sub-nodes:

- **Server Options** - Provides access to all configuration settings of the DeviceLock Content Security Server. For further details, see [Server Options](#).
- **Search Server** - Provides access to Search Server functions. For further details, see [Using Search Server](#).
- **Discovery Server** - Provides access to Discovery Server functions. For further details, see [DeviceLock Discovery Overview](#).

## Server Options

Use this node to configure the DeviceLock Content Security Server. The administrator can configure the following settings:

- **Server Administrators** - Specify the server administrators and their associated access rights. For further details, see [Server Administrators](#).
- **Search Server Options** - Configure full-text search related settings. For further details, see [Search Server Options](#).
- **Discovery Server Options** - Configure content discovery settings for Discovery Server.
- **Alerts** - Configure alerts delivery settings for Discovery Server.
- **DeviceLock certificate** - Install, change or remove the DeviceLock certificate.
- **Service startup account** - Specify the startup account information, such as the account name and the password, for the server service.
- **TCP port** - Specify the TCP port to connect the DeviceLock Management Console to the server.
- **Connection type** - Choose the ODBC driver or system data source to connect to the DeviceLock Content Security Server's database.
- **SQL Server name** - Specify the DeviceLock Content Security Server's database server. This setting is available for the ODBC driver connection type.
- **System Data Source** - Specify the data source to access the DeviceLock Content Security Server's database server. This setting is available for the system data source connection type.
- **Database name** - Specify the name of the DeviceLock Content Security Server's database.
- **SQL Server login** - Specify the login and password to access the DeviceLock Content Security Server's database. This setting is available for the SQL Server Authentication mode.

The shortcut menu on this node provides the following command:

- **Properties** - Starts the wizard for managing server options.

For further details, see [Managing General Settings](#).

## Server Administrators

The **Server Administrators** node determines the list of server administrators and their rights on the DeviceLock Content Security Server, and the DeviceLock certificate used by that server.

The shortcut menu on this node provides the following command:

- **Properties** - Opens a dialog box to set up the list of server administrators, and install or remove a DeviceLock certificate.

See also:

[Configuring access to the DeviceLock Content Security Server](#)

[Installing or removing a DeviceLock certificate](#)

[Server administrators and certificate](#)

## Search Server Options

Use this node to configure Search Server. The administrator can configure the following settings:

- **DeviceLock Enterprise Server(s)** - Specify the DeviceLock Enterprise Server/s whose data will be indexed for full-text search.
- **Index directory** - Specify the location of the full-text index.
- **Indexing interval** - Specify the time interval, in minutes, between the end of one indexing process and the start of the next indexing process.
- **Merge Interval** - Specify the time interval, in minutes, at which to perform index merge operations.
- **Extract text from binary files** - Choose whether to index text data from non-text (binary) files.
- **Extract text from images (OCR)** - Choose whether to index text data found on images by using Optical Character Recognition (OCR). Up to 8 languages for OCR can be selected.

---

### Note

Selecting multiple Asian languages (marked with an asterisk (\*) in the GUI) or selecting an Asian language together with non-Asian languages may cause performance degradation of the OCR engine.

---

- **Search Server License(s)** - Install the required number of Search Server licenses.
- **Notification Settings** - Specify the e-mail (SMTP) server for sending Search Server reports.

For further details, see [Managing Search Server Settings](#).

## Managing General Settings

There are three types of configuration settings for the DeviceLock Content Security Server:

- **General settings** - Affect the operation of the DeviceLock Content Security Server as a whole. The current section provides instructions for managing these settings.
- **Search Server settings** - Affect the operation of the Search Server, a part of the DeviceLock Content Security Server. For management instructions, see [Managing Search Server Settings](#).
- **Discovery Server settings** - Affect the operation of the Discovery Server, a part of the DeviceLock Content Security Server. For details, see [Discovery Server Options](#).

The administrator can configure general server settings when installing the DeviceLock Content Security Server, or use the DeviceLock Management Console to configure and/or modify them after the server has been installed and is functioning.

---

**Note**

- Only server administrators with sufficient rights can manage and use the DeviceLock Content Security Server.
  - To begin, connect the DeviceLock Management Console to the computer running the DeviceLock Content Security Server: Right-click **DeviceLock Content Security Server**, and then click **Connect**. For more information, see [Connecting to Computers](#).
- 

With the DeviceLock Management Console, the administrator can perform the following server configuration tasks:

- Configure which users have access to the DeviceLock Content Security Server.
- Change the startup account information, such as the account name or the password, for the DeviceLock Content Security Server service.
- Install or remove the DeviceLock certificate to authenticate communications between the DeviceLock Content Security Server and the DeviceLock Enterprise Server.
- Change the TCP port to connect the DeviceLock Management Console to the DeviceLock Content Security Server.
- View or change the DeviceLock Content Security Server's database connection settings.

One can perform these tasks individually or collectively.

To perform the tasks collectively, use the DeviceLock Content Security Server configuration wizard. This is the wizard that starts automatically when installing or upgrading the DeviceLock Content Security Server.

**To perform configuration tasks collectively**

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, right-click **Server Options**, and then click **Properties**.  
*The first page of the wizard appears.*
3. Move through the wizard pages. After completing each page, move to the following one by clicking **Next**, or move to the preceding one by clicking **Back**. On the final page, click **Finish** to complete the wizard.  
For description of the wizard pages, see the [Perform Configuration and Complete Installation](#) section in the [Installing DeviceLock Content Security Server](#) instruction.

Using the DeviceLock Management Console, the administrator can perform the following tasks to configure individual server settings:

- [Configuring access to the DeviceLock Content Security Server](#)
- [Setting the service startup account](#)
- [Installing or removing a DeviceLock certificate](#)

- [Configuring the TCP Port setting](#)
- [Managing the database connection settings](#)

## Configuring access to the DeviceLock Content Security Server

The administrator can specify the users who are allowed to access the DeviceLock Content Security Server. This restricts outsiders from accessing or damaging the server.

### *To configure which users have access to the server*

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, do one of the following:
  - Select **Server Options**. In the details pane, double-click **Server Administrators** or right-click **Server Administrators** and then click **Properties**.  
- OR -
  - Expand **Server Options**. Under **Server Options**, right-click **Server Administrators** and then click **Properties**.

3. In the **DeviceLock Content Security Server** dialog box that appears, do the following:

#### **To enable default security**

- Select the **Enable Default Security** check box.

If default security is enabled, members of the local Administrators group will have full access to the DeviceLock Content Security Server.

#### **To restrict access to the server to specific users**

- a. Clear the **Enable Default Security** check box.
- b. Under **Users**, click **Add** to add the specific users to be allowed access to the DeviceLock Content Security Server.
- c. In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.  
The selected users/groups become server administrators, which are listed under **Users** in the **DeviceLock Content Security Server** dialog box. Server administrators are authorized to perform the tasks related to configuring and using the DeviceLock Content Security Server and, by default, they have full access to the server.

To change the server access level for a particular administrator, select the respective user or group under **Users**, and then choose from the following options in the list of access rights:

- **Full access** - Allows the user or group to install and uninstall the DeviceLock Content Security Server, connect to it by using the DeviceLock Management Console, and perform any actions on the server, such as: view and change server settings; create and run search queries and tasks; view and change content detection settings; create and run discovery tasks and reports.
- **Change** - Same as full access to the server with the exception of the right to make changes to the list of server administrators or change the level of access to the server for the users or groups already in that list.
- **Read-only** - Allows the user or group to connect to the DeviceLock Content Security Server by using the DeviceLock Management Console; view server settings; run search queries; view and



run existing search tasks; view content detection settings; view discovery reports and manually create new reports based on the existing reports and data already prepared by discovery tasks. This option does not give the right to run discovery tasks, make any changes on the server, or create a new index for the Search Server.

For users and groups with **Change** or **Read-only** access, the **Shadow Data Access** option can be selected to allow access to shadow copies and user activity records. The users and groups with this option selected are allowed to search the content of shadow copies and user activity records, and open, view, and save shadow copies and user activity records from search results. Without access to shadow data, DeviceLock Content Security Server administrators cannot open, view, or save shadow copies and records of user activity. Search results do not have the **Open**, **Save**, and **View** links, and asterisks are displayed instead of text snippets of shadow copies and user activity records. Logins and passwords in document parameters for user activity records are also replaced with asterisks.

---

#### Note

We strongly recommend that administrators of DeviceLock Content Security Server be given local administrator rights.

---

To revoke server administrator rights from a particular user or group, select that user or group in the **Users** area, and then click the **Delete** button.

One can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

4. Click **OK**.

## Setting the service startup account

Over time, the administrator might need to change the account that was specified as the service startup account when installing the DeviceLock Content Security Server. It is also possible to change the password of the service startup account.

### *To change the service startup account or password*

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options**.
3. In the details pane, double-click **Service startup account** or right-click **Service startup account** and then click **Properties**.
4. In the **DeviceLock Content Security Server** dialog box that appears, do the following:  
**To change the service startup account**
  - a. In the **Log on as** area, click **Browse**.
  - b. In the **Select User** dialog box that appears, in the **Enter the object name to select** box, type the name of the user, and then click **OK**.  
The selected user is displayed in the **This account** box in the **DeviceLock Content Security Server** dialog box.

We recommend the use of an account with administrator rights on all computers running the DeviceLock Enterprise Server. In an Active Directory environment, we recommend the use of an account that is a member of the Domain Admins group. Otherwise, DeviceLock certificate authentication should be used.

**To change the service account password**

- a. In the **Log on as** area, type a new password in the **Password** box.
- c. Re-type the new password in the **Confirm password** box.

**To assign the Local System account to the server service**

- In the **Log on as** area, click **Local System account**.

---

**Important**

As the Local System account cannot be used to authenticate when connecting to the DeviceLock Enterprise Server on remote computers, DeviceLock certificate based authentication must be used in this case.


---

5. Click **OK**.

## Installing or removing a DeviceLock certificate

If the service startup account of the DeviceLock Content Security Server cannot authenticate with the remote DeviceLock Enterprise Server, DeviceLock certificate authentication can be used. To use this kind of authentication, install the private key of the same DeviceLock certificate on both the DeviceLock Content Security Server and DeviceLock Enterprise Server. For details on DeviceLock certificates, see [DeviceLock Certificates](#).

***To install or remove a DeviceLock certificate on the DeviceLock Content Security Server***

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options**.
3. In the details pane, double-click **DeviceLock certificate** or right-click **DeviceLock certificate** and then click **Properties**.
4. In the **DeviceLock Content Security Server** dialog box that appears, do the following:
  - To install the private key of the DeviceLock certificate**
    - a. Next to the **Certificate Name** box, click the  button to open the **Select the DeviceLock Certificate file** dialog box and browse for the file to use.
    - b. In the **Select the DeviceLock Certificate file** dialog box, locate and select the certificate file, and then click **Open**.

The certificate name appears in the **Certificate Name** box of the **DeviceLock Content Security Server** dialog box.
  - To remove the private key of the DeviceLock certificate**
    - Next to the **Certificate Name** box, click **Remove**.
5. Click **OK**.

## Configuring the TCP Port setting

Over time, the administrator might need to change the TCP port that the DeviceLock Management Console uses to connect the DeviceLock Content Security Server.

### *To change the TCP port for connecting the console*

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options**.
3. In the details pane, double-click **TCP port** or right-click **TCP port** and then click **Properties**.
4. In the **Connection Settings** area of the **DeviceLock Content Security Server** dialog box that appears, do one of the following:
  - Click **Dynamic ports** to use a dynamic port selection.  
- OR -
  - Click **Fixed TCP port** to use a specified port. Then, type the desired port number in the **Fixed TCP port** box.  
By default, the DeviceLock Content Security Server uses TCP port 9134.
5. Click **OK**.

## Managing the database connection settings

A database connection is required for the Search Server and Discovery Server to function. If there is no connection to the database, it is impossible to search using content-aware groups, save and automate search queries, or use the Discovery Server for content discovery.

### *To view or change the database connection settings*

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options**.
3. In the details pane, double-click any of these options: **Connection type**, **SQL Server name**, **Database name**, or **SQL Server login**. Alternatively, right-click an option, and then click **Properties**.
4. In the dialog box that appears, view or change the following connection settings:
  - **Database name** - The name of the DeviceLock Content Security Server's database.
  - **Connection type** - Determines whether to use an ODBC driver or system data source to connect to the DeviceLock Content Security Server's database server.  
Further options depend upon the selected connection type.
  - **SQL Server name** - The name of the database server (if using an ODBC driver).  
Empty name indicates a database server running on the same computer as the DeviceLock Content Security Server.
  - **Windows authentication / SQL Server authentication** - The authentication mode to use on SQL Server (for Microsoft SQL Server ODBC driver).
  - **Data source name** - The name of the system data source (if using a system data source).

- **Login name, Password** - Login and password to access the database (if using the SQL Server Authentication mode).

5. Click **Next**, wait while the console completes the connection, and then click **Finish**.

For details on the database connection settings, see the [Database settings](#) section in the [Installing DeviceLock Content Security Server](#) instruction.

## Managing Search Server Settings

Search Server settings apply to the Search Server component of the DeviceLock Content Security Server. When installing the DeviceLock Content Security Server, it is only possible to install Search Server licenses. Use the DeviceLock Management Console to administer all Search Server settings.

This section provides instructions on how to perform the following configuration tasks:

- [Installing Search Server licenses](#)
- [Specifying DeviceLock Enterprise Server/s to index](#)
- [Specifying Search Server index location](#)
- [Setting up the index to include text data from binary files](#)
- [Setting up indexing schedule](#)
- [Setting up merge operations schedule](#)
- [Rebuilding the index on demand](#)
- [Updating the existing index on demand](#)
- [Checking the status of the current indexing actions](#)
- [Specifying mail server for Search Server reports](#)

## Installing Search Server licenses

A special Search Server license must be purchase for the DeviceLock Content Security Server. The same license can be used on an unlimited number of computers running the DeviceLock Content Security Server.

Search Server licensing is based on the number of log entries to be indexed for full-text search. Each license allows the indexing of 1,000 entries in the Shadow Log (including shadow copies), 1,000 entries in the UAM log (including keyboard input records), and 5,000 entries in each of the other logs (Audit Log, Deleted Shadow Data Log, Server Log, Monitoring Log, and Policy Log).

Depending upon the actual number of log entries on their DeviceLock Enterprise Server/s, the organization can purchase as many licenses as required. If using several licenses, the Search Server can index as many log entries as the total license count allows. It is always possible to purchase and install additional Search Server licenses. The trial period for the DeviceLock Content Security Server is 30 days. During the trial period, the Search Server can index 2,000 entries in the Shadow Log, 2,000 entries in the UAM Log, and 10,000 entries in each of the other logs.

### ***To install Search Server licenses***

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.
3. In the details pane, double-click **Search Server License(s)** or right-click **Search Server License(s)** and then click **Properties**.
4. In the **DeviceLock Content Security Server** dialog box that appears, click **Load License(s)**.
5. In the dialog box that appears, locate and select the license file, and then click **Open**.  
*Having loaded the license files, the administrator can view the license information summary where Total license(s) displays the total number of purchased licenses while Used license(s) displays the number of licenses currently in use for indexing log data.*  
*The administrator can install as many licenses as required to suit the organization's needs, by loading license files one by one.*
6. Click **OK**.

## Specifying DeviceLock Enterprise Server/s to index

To start the search index creation, there must be specified the DeviceLock Enterprise Server/s to index. The indexing starts automatically as soon as the DeviceLock Enterprise Server/s have been specified.

### To specify DeviceLock Enterprise Server/s

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.
3. In the details pane, double-click **DeviceLock Enterprise Server(s)** or right-click **DeviceLock Enterprise Server(s)** and then click **Properties**.

*The DeviceLock Enterprise Server(s) dialog box appears.*



4. In the **DeviceLock Enterprise Server(s)** dialog box, type the IP address or the name of the computer running the DeviceLock Enterprise Server.  
*Multiple computer names or IP addresses must be separated by a semicolon (;).*

---

**Note**

Make sure that the DeviceLock Enterprise Server is properly installed and can be accessed by the DeviceLock Content Security Server; otherwise, its log data will not be indexed by the Search Server.

---

To remove computer names or IP addresses, click **Remove**.

5. Click **OK**.

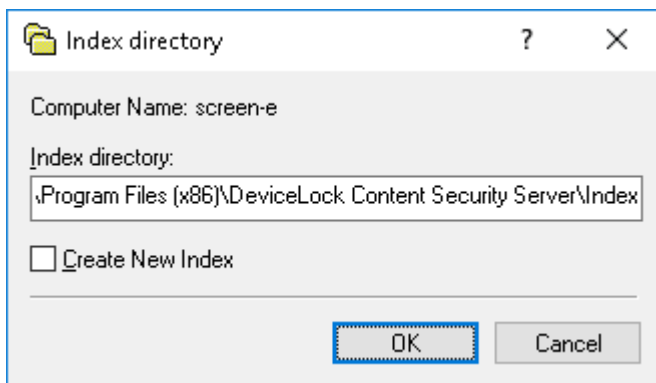
## Specifying Search Server index location

The administrator can specify the folder to hold the search index, referred to as the index location. If the folder is not specified, the index is located in the default folder %ProgramFiles%\DeviceLock Content Security Server\Index. The Search Server starts the indexing process automatically each time the index location changes.

### ***To specify the index location***

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.
3. In the details pane, double-click **Index directory** or right-click **Index directory** and then click **Properties**.

*The Index directory dialog box appears.*



4. In the **Index directory** box, type the path to the desired folder.  
To create a new index immediately, select the **Create New Index** check box.

*If the index already exists at the specified location and creating a new index is chosen, the following message appears: "Do you want to create the new index and overwrite the existing one (Yes - Overwrite, No - Append)?" In the message box, click Yes to completely rebuild the index immediately. Click No to update the existing index with changes immediately.*

5. Click **OK**.

## Setting up the index to include text data from binary files

The administrator can enable or disable the extraction and indexing of text data from binary, non-text files.

### ***To enable or disable the extraction of text data from binary files***

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.
3. In the details pane, double-click **Extract text from binary files** or right-click **Extract text from binary files**, and then click **Enable** or **Disable**.

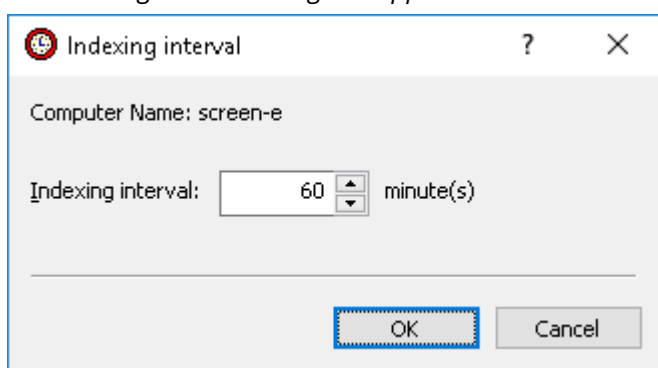
## Setting up indexing schedule

The Search Server provides for the creation and update of the search index on a schedule. The indexing schedule is based on the indexing interval that is a time interval between the end of an ongoing indexing session and the beginning of the next indexing session. The default indexing interval is 60 minutes.

### ***To configure the indexing schedule***

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.
3. In the details pane, double-click **Indexing interval** or right-click **Indexing interval** and then click **Properties**.

*The Indexing interval dialog box appears.*



4. In the **Indexing interval** box, type or select the desired number of minutes for the indexing interval.
5. Click **OK**.

## Setting up merge operations schedule

By performing the index merge on a schedule, the Search Server aggregates temporary indexes into an operational index to serve search queries. The schedule is based on the merge interval that determines how often to update the operational index with new data from the temporary indexes. The merge interval can be set from 1 to 100,000 minutes. The default value is 10 minutes.

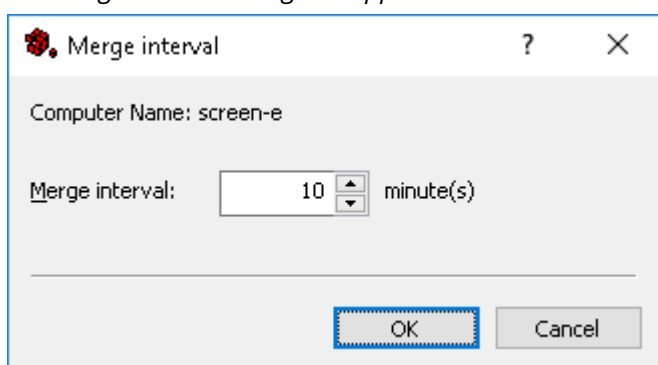
When deciding on the merge interval value, consider the following:

- The shorter the merge interval, the faster the index merge is completed.
- The server cannot perform search queries until the index merge is complete.

### ***To configure a schedule for merge operations***

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Server Options**.
2. Under **Server Options**, select **Search Server Options**.
3. In the details pane, double-click **Merge Interval** or right-click **Merge Interval** and then click **Properties**.

*The Merge interval dialog box appears.*



4. In the **Merge interval** box, type or select the desired number of minutes for the merge interval.
5. Click **OK**.

## Rebuilding the index on demand

The administrator can completely rebuild the full-text index immediately.

### ***To rebuild the full-text index immediately***

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, right-click **Search Server**, and then click **Create New Index**.

*If the index already exists and creating a new one is requested, the following message appears: "Do you want to create the new index and overwrite the existing one (Yes - Overwrite, No - Append)?" In the message box, click Yes to completely rebuild the index immediately. Click No to update the existing index with changes immediately.*

## Updating the existing index on demand

In case of a need to urgently index new data that appeared on the DeviceLock Enterprise Server, the administrator can immediately update the existing index with this new data, without waiting for a scheduled update of the index.

### ***To update the existing index immediately***



1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, right-click **Search Server**, and then click **Index Now**.

*During an update operation, the Search Server does not perform a full rebuild of the index. It indexes only new data on the DeviceLock Enterprise Server in order to add new index entries to the existing index.*

## Checking the status of the current indexing actions

The administrator can use the **Current Activity** node to monitor the status of the current indexing actions.

Full-text indexing operations can be time-consuming and resource-intensive. The Search Server enables the administrator to monitor the progress of the indexing operations being performed.

The indexing process is performed in two stages. First, the Search Server extracts significant words from shadow copies and log records and saves them to temporary indexes per DeviceLock Enterprise Server instance. For each temporary index, the Search Server processes 1,000 records from each log.

In the second stage, when either the number of temporary indexes becomes equal to 50, or 10 minutes pass, all temporary indexes are combined into a permanent master index that is used for search queries. The process of combining temporary indexes into a master index is called *merging*.

When **Current Activity** is selected in the console tree, the details pane displays the indexing and merging status and progress indicators.

### ***Indexing status and progress indicators***

The administrator can control the indexing process for each specified DeviceLock Enterprise Server by watching its status and progress indicators. The status indicator shows the current status of the indexing operation:

Status	Description
Idle	Indexing is not performed.
Waiting	Waiting for indexing to begin.
Indexing <log_name>	Indexing the specified log is in progress.

The progress indicator shows the percentage complete of the indexing process.

### ***Merging status and progress indicators***

The administrator can control the merge process by watching its status and progress indicators. The status indicator shows the status of the merge operation:

Status	Description
Idle	The merge is not performed.



Merging	The merge is in progress.
Defragmenting	Compressing and optimizing the index by removing obsolete index data and consolidating search structures for better performance.

The progress indicator shows the percentage complete of the merge process.

### ***To monitor the status of the indexing and merge process***

1. In the console tree, expand **DeviceLock Content Security Server**, and then expand **Search Server**.
2. Under **Search Server**, select **Current Activity**.

When **Current Activity** is selected in the console tree, the details pane displays the indexing and merging status and progress indicators. Since the indicators are not updated automatically, refresh them by hand:

- Right-click **Current Activity**, and then click **Refresh**.  
- OR -
- Select **Current Activity**, and then click  on the toolbar.  
- OR -
- In the details pane, right-click any name of the DeviceLock Enterprise Server or **Merge Index**, and then click **Refresh**.  
- OR -
- In the details pane, select any name of the DeviceLock Enterprise Server or **Merge Index**, and then click  on the toolbar.

## Specifying mail server for Search Server reports

The Search Server uses a mail (SMTP) server to deliver reports containing search results. The administrator can specify the mail server by using the **Notification Settings** command on the shortcut menu of the **Search Server** node or by using the **Notification Settings** option in the **Search Server Options** node.

### ***To specify the mail server for delivering Search Server reports***

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, right-click **Search Server**, and then click **Notification Settings**. Alternatively, expand **Server Options**, select **Search Server Options**, and then double-click **Notification Settings** in the details pane.
3. In the dialog box that appears, select the **Use e-mail notifications for reports** check box, and specify the following settings:
  - **SMTP host** - Specify the SMTP server to send reports. In this field, enter the name or IP address of the server.
  - **Port** - Specify the port for connecting to the SMTP server. The default port is 25. Clear the **Default** check box to enter a different port number.

---

**Note**

DeviceLock supports both unencrypted and SSL-encrypted connections to the SMTP server. The connection type is set automatically, depending upon whether SSL is enabled on the SMTP server.

---

- **Server requires authentication** - Select this check box if authentication is required to connect to the SMTP server specified. Otherwise, leave this check box cleared.  
If the **Server requires authentication** check box is selected, the **User name** and **Password** fields must specify the name and password of an e-mail account that has permission to connect to the SMTP server.
  - **Sender Address** - Supply the address to display in the **From** field of the e-mail messages with Search Server reports.
4. Optionally, click **Test** to verify the mail server settings.
  5. In the dialog box that appears after clicking **Test**, specify the address of the mail recipient, and click **OK** to send a test message via the mail server specified.  
In case of valid mail server settings, the message is delivered to the recipient. Otherwise, the console displays an error message describing the problem.
  6. When finished, click to **OK**.

## Using Search Server

A part of the DeviceLock Content Security Server, the Search Server enables the full-text searching of log data stored on the DeviceLock Enterprise Server. Search queries can include text fragments to find as well as so-called search groups to search by various features of data, such as file types, keywords, or document properties (see [Managing content-aware search groups](#)). All these search capabilities simplify and make more efficient the analysis of large amounts of data accumulated in the DeviceLock Enterprise Server logs.

The shortcut menu on the **Search Server** node provides the following commands:

- **Create New Index** - Immediately begins to rebuild the entire search index. For details, see [Rebuilding the index on demand](#).
- **Index Now** - Immediately begins to update the existing search index. For details, see [Updating the existing index on demand](#).
- **Notification Settings** - Specifies the mail (SMTP) server to deliver reports. For details, see [Specifying mail server for Search Server reports](#).

Using Search Server involves:

- [Performing a search](#)
- [Working with search results](#)
- [Automating search operations](#)

## Performing a search

With the Search Server, one can find all the DeviceLock Enterprise Server log records in which a certain word or text fragment occurs. Since search queries usually return a large number of results, the Search Server provides a number of options to fine tune and optimize the search. These options make it possible to specify exactly what search results should be returned.

Using search options, one can:

- Filter search results by date, log, sender, recipient, file type, source, etc. Thus, using a filter, one could limit search results to certain logs and a given date range.
- Set the number of search results per page.

For a description of the search options along with instructions on setting up and executing a search, see [Steps to perform a search](#).

Having completed a search, the server returns a search results page, divided into the following view areas:

- [Search query](#) - Displays the search criteria that were used by the search.
- [Statistics bar](#) - Shows the number of results displayed on the current search results page.
- [Search results](#) - Displays a numbered list of items containing information that matched the search criteria.
- [Results navigator](#) - Shows how many results pages are returned, and allows one to navigate from page to page.

For more information, see [Working with search results](#).

Here are some notes to consider when using full-text search:

- It is possible to search individual fields that appear in the **Log Parameters** and **Document Parameters** sections of a search result. For such a search, use the following syntax: `<field name>::<value>`. For example: `File Name::Prices.docx`.  
You can search by multiple field name-value pairs, having enclosed each pair in parentheses. For example, a search for `(File Name::secret) (File Type::Excel)` will return Excel files that contain the word `secret` in the file name.

---

### Important

Field names should be specified case-sensitive. The lowercase and uppercase letters in the field name are considered different.

---

- Searching the UAM Log also searches keyboard input records. It is possible to search for fragments of text and for passwords that the user entered. Passwords are searched for by the value of the Passwords field in user activity records: `Passwords::<value>`. For example, you can use the following syntax to find records that contain any passwords: `Passwords::?* (an asterisk without a question mark would match any password or no password)`.

- Search request string can include logical operators, such as AND and OR. A space between words is equivalent to AND. A semicolon (;) is equivalent to OR. Logical operators must be typed uppercase. For further details, see [About logical operators](#).
- Search request string is not case sensitive except for search by field value. Field names are case-sensitive.
- Stemming is enabled by default. Stemming extends a search to cover grammatical variations on a word. Thus, the request `applied` would also retrieve `applying`, `applies`, and `apply`. Stemming is supported for English, French, German, Italian, Portugal, Russian, and Spanish.
- Search request string can include wildcard characters such as asterisks (\*) and question marks (?). An asterisk denotes any series of characters or no characters. The question mark denotes any single character. You can use any number of wildcard characters in any position.
- To search for a specific phrase, enclose the phrase in double quotes in the search request string. To search for multiple words, separate each word with a space.

The following table shows the search items, examples, and results of different search types.

Search item	Example	Results
Single word	price	Results that contain the word <code>price</code> . The search will also find grammatical variations, such as <code>prices</code> , <code>priced</code> , and so on.
Phrase	confidential information	Results that contain both of the individual words <code>confidential</code> and <code>information</code> , rather than the exact phrase.
	"confidential information"	Results that contain the exact phrase <code>confidential information</code> .
Wildcard search	te?t	Results that contain <code>test</code> , <code>text</code> , and so on.
	mone*	Results that contain <code>money</code> , <code>monetary</code> , and so on.
	*air	Results that contain <code>air</code> , <code>fair</code> , <code>impair</code> , <code>affair</code> , and so on.
	"* assets"	Results that contain phrases ending with <code>assets</code> , such as <code>monetary assets</code> , <code>liquid assets</code> , <code>fixed assets</code> , <code>current assets</code> .
Boolean search  See also <a href="#">About logical operators</a>	price AND quality	Results that contain both <code>price</code> and <code>quality</code> .
	price quality	
	price OR quality	Results that contain either <code>price</code> or <code>quality</code> , or both of these words.
	price; quality	
Search by	(Action::Message) (Recipient::	All e-mail messages with <code>.pdf</code> and <code>.doc</code>

field	john.smith@domain.com) (Attachments::doc) (Attachments::pdf)	attachments sent to john.smith@domain.com.
	(Action::Chat) (File Name::Mike)	All instant messages sent to/from the user Mike.
	(File Name::secret) (File Type::Excel)	Excel files with the name containing secret, transmitted via any supported channel.
	(File Type::Acrobat) (Source::File Sharing) (File Size::100~~200 MB)	PDF files of the size between 100 and 200 MB, uploaded to file sharing sites or downloaded from such sites.

Moreover, the Search Server supports advanced syntax in search query strings.

Character	Meaning	Description
=	any single digit	N=== would match N123 but not N1234 or Nabc.
-	exclude	Put - (dash) in front of a word or phrase to exclude it from search results. E.g. -"monetary assets"
%	fuzzy search	Fuzzy searching will find a word even if it is misspelled. The number of the added characters % determines the number of differences ignored when searching for a word. The position of the characters % determines how many characters at the beginning of the word have to match exactly. Fuzzy searching can be useful when searching text that contains misspelled words. E.g. inf%%ormation would find words beginning with inf and spelled with no more than two differences from the word information.
#	phonic search	Phonic searching looks for a word that sounds like the given word and begins with the same letter. Phonic searching is somewhat slower than other types of searching and tends to make searches over-inclusive. For the English language only. E.g. #smith would find smithe and smythe.
&	synonym search	Synonym searching finds synonyms of the word specified in the search request. For the English and Russian languages only. E.g. fast& would also find quickly.
~~	numeric range	A numeric range search is a search for any numbers that fall within a range. To add a numeric range to a search request, enter the upper and lower bounds of the search separated by ~~. A numeric range search includes the upper and lower bounds. Decimal points and commas are treated as spaces and minus signs are ignored. E.g. 500~~1000 would find text containing numbers between 500 and 1000.
:	variable term weighting	By default all words in a request count equally in counting hits. However, this can be changed by specifying the relative weights for each term in the search request. E.g. money:5 information:1 would retrieve the same documents as money information but the Search Server would weight money five times as heavily as information when sorting the results.

##	regular expression	Regular expressions provide a way to search for complex combinations of characters. In a search request, a regular expression must be enclosed in double quotes and must begin with ##. Search Server employs the TR1 implementation of regular expressions (for details, see <a href="https://msdn.microsoft.com/library/bb982727.aspx">msdn.microsoft.com/library/bb982727.aspx</a> ). A regular expression can only match a single word or group of digits. No case conversion is done on regular expressions, so a regular expression must match the case of the string data stored in the index. The search speed depends on the placement of the regular expression in the search query: the closer the expression is to the beginning of the word, the longer the search takes.
----	--------------------	--

## About logical operators

The Search Server supports “Boolean” search requests where words or expressions are united by logical operators such as AND or OR. Examples:

- price AND quality - Both words must be present.
- price OR quality - At least one of these words must be present.
- price W/3 quality - The word “price” must occur within 3 words of the word “quality”.
- price NOT W/3 quality - The word “price” must occur, but not within 3 words of the word “quality”.
- price AND NOT quality - The word “price” must be present whereas the word “quality” must be missing.

In the case of more than one operator, use brackets to avoid ambiguity of the search request. For example, the request price AND quality OR quantity could mean (price AND quality) OR quantity, or it could mean price AND (quality OR quantity). For best results, always enclose expressions with logical operators into brackets.

The following logical operators are supported:

- [AND/OR operators](#)
- [W/N and PRE/N operators](#)
- [NOT and NOT W/N operators](#)

## AND/OR operators

Use the AND operator to combine two words or expressions, both of which must be present in every search result.

Use the OR operator to combine two words expressions, at least one of which must be present in every search result.

### **W/N and PRE/N operators**

Use the W/N operator to specify that one word or phrase must occur within N words of the other. For instance, the request price W/3 quality would return results that contain the word “price” within 3 words of the word “quality”.

The PRE/N operator is like W/N but also specifies that the first expression must precede the second one. For instance, the request `price PRE/3 quality` would return results that contain the word “price” at most 3 words before the word “quality”.

To avoid ambiguity of the search request, at least one of the two expressions united by W/N or PRE/N should be a single word or phrase, or a group of words and phrases united by OR.

The identifier `xfirstword` is provided to mark the first word of a search item. In conjunction with the W/N operator, this identifier enables searching for certain words or expressions in the vicinity of the item’s beginning. For instance, the request `price W/3 xfirstword` would return results that contain the word “price” within 3 words of the first word in a message or file.

### **NOT and NOT W/N operators**

Use the NOT operator at the beginning of the expression to reverse its meaning. This allows the items matching the expression to be excluded from the search results.

The NOT operator can be put at the beginning of the search request. In this case, it reverses the meaning of the entire request. For instance, the request `NOT (price W/3 quality)` would return results that do not contain the word “price” within 3 words of the word “quality”.

If the NOT operator is used between expressions, then it should be supplemented with another operator, such as AND or OR. Thus, the request `price AND NOT quality` would return results that contain the word “price” and do not contain the word “quality”.

The combination of the NOT and W/N operators (meaning “not within”) can be used to search for a word or phrase not in association with another word or phrase. For instance, the request `price NOT W/3 quality` would return results that contain the word “price”, but not within 3 words of the word “quality”. Note that unlike the W/N operator, NOT W/N is not symmetrical, so the request `price NOT W/3 quality` is not the same as the request `quality NOT W/3 price`.

## **Steps to perform a search**

Use the following steps to configure and perform a search:

1. In the console tree, select **DeviceLock Content Security Server > Search Server > Search Page**.  
*As a result, the details pane displays the search page.*
2. On the search page, in the **Search** box, specify the query string to search for the desired words or expressions.  
When composing a query string, one can use commands from the shortcut menu that appears upon a right-click in the **Search** box:
  - **Insert** - Point to this menu item and then choose to add a logical operator, a saved query string, or a content-aware search group to the **Search** box:
    - Adding a logical operator - Add operators such as AND/OR by typing them in uppercase, or by choosing an operator from the **Insert** menu. For details, see [About logical operators](#).
    - Adding a saved query - Use the **Saved Query** command to add a previously saved query string. For details, see [Managing saved queries](#).



- Adding a search group - Use the **Content-Aware Group** command to add a content-aware search group. For details, see [Managing content-aware search groups](#).  
In the **Search** box, a search group is presented by its name enclosed in percent signs: %group\_name%. One could add a search group by typing a percent sign followed by the group name.
  - **Save as** - Saves the current query string for future reuse. For more information, see [Managing saved queries](#).
3. To set search options, click **Options** and then do the following:
- To specify the number of search results to display per page, in the **Display <number> results per page** list, click any of the following options: **10, 20, 30, 50, 100**. The default number of returned results is 20.
  - To search only selected logs, select the check box next to each desired log under **Limit results to the following logs**.  
*By default, the following logs are selected: Audit Log; Shadow Log; Deleted Shadow Data Log.*
  - To search log records by date, use the options to specify the desired date range:
    - **From** - The beginning of the date range. Possible values:
      - **First Record** - Search records starting from the earliest one in the log. This is the default value.
      - **Records On** - Search records logged after or on a selectable date.
    - **To** - The end of the date range. Possible values:
      - **Last Record** - Search records up to the latest one in the log. This is the default value.
      - **Records On** - Search records logged before or on a selectable date.

If selecting **Records On**, click in the **From** or **To** field to open the calendar. In the calendar, click to select the desired date. Use the arrows < | > to change the month and double arrows << | >> to change the year.

  - To search log records by sender, recipient, file type, device type, or protocol, use the options under **Limit results to the following parameters**:
    - **Sender(s)** - Sender identifiers for the following protocols: IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMTP, Telegram, Viber, Web Mail, WhatsApp, Zoom. The search returns the results associated with the specified sender/s.
    - **Recipient(s)** - Recipient identifiers for the protocols IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMTP, Telegram, Viber, Web Mail, WhatsApp, Zoom, as well as for the following social networks: Facebook, Google+, LiveJournal, LinkedIn, LiveInternet, Myspace, Odnoklassniki, Twitter, VKontakte. The search returns the results associated with the specified recipient/s.
    - **File Type(s)** - A description of the desired file type/s (either full or partial), for example: E-Mail message (Var.2), Disk Image (Macintosh), Zip 1.0. The search returns the results associated with the specified file type/s.
    - **Source(s)** - The desired device type/s or protocol/s. The search returns the results associated with the specified type/s of device or specified protocol/s.

The **Sender(s)**, **Recipient(s)**, and **File Type(s)** fields allow the use of an asterisk (\*) to denote any series of characters and a question mark (?) to denote any single character, as well as the use of the logical operators AND (space) and OR (semicolon ;).

4. Click **Search**.

## Managing saved queries

When performing a full-text search or setting up a search task, there must be specified a query string to search for specific words or text fragments. Since the creation of such a query string “from scratch” can be time-consuming and error-prone, the Search Server provides the option to save and reuse search queries.

Query strings can be saved from the **Search** box (see [Steps to perform a search](#)): Right-click in the **Search** box, click **Save As**, and specify a query name in the dialog box that appears. Another way to open that dialog box: Right-click in the **Search** box, point to **Insert**, and click **Saved Query**.

Query strings can also be saved from the **Query** field for a search task (see [Setting up the search query](#)): Right-click in the **Query** field, click **Save As**, and specify a query name in the dialog box that appears. Another way to open that dialog box: Click **Saved Query** next to the **Query** field.

The dialog box for managing saved queries lists all saved queries that are available on the server, and allows one to:

- **Create a new saved query** - Click the **New** button, and specify the query string in the same way as when setting up a query for a search task or full-text search.
- **View or change a saved query** - Select the query from the list, click the **Edit** button, and then view or change the query string in the dialog box that appears.
- **Change the name of a query** - Select the query, and click the **Rename** button. Then, type a new name in the list.
- **Delete a query** - Select the query, and click the **Delete** button.
- **Export all saved queries to a file** - Click the **Save** button, and specify the export file to store the queries.
- **Import queries from an export file** - Click the **Load** button, and select the export file.

## Creating or editing a saved query

When creating, viewing, or changing a saved query, a separate dialog box appears to manage that query.

In the **Query** field of the dialog box for managing a saved query, specify one or more query strings to search for the desired words or text fragments, in the same way as you do in the **Query** field when configuring a search task or in the **Search** box when performing a full-text search. By default, the strings are combined by AND, that is, the query would return the items that match each of the strings specified.

In the query string, logical operators, such as AND or OR, can be added by typing them in uppercase, or by choosing an operator from the shortcut menu. To display the menu, right-click in the **Query**

box and point to **Insert**, or click in the **Query** box and then press Ctrl+D. For operator description, see [About logical operators](#).

The query string can include search groups (see [Managing content-aware search groups](#)). A search group is presented by its name enclosed in percent signs: %group\_name%. It is possible to add a search group to the query string by typing percent signs along with the group name. As you type, a list of groups that match the entered name appears in the **Query** box, allowing you to select the desired group from that list.

The shortcut menu in the **Query** box also provides the standard commands for working with text, such as **Cut**, **Copy**, **Paste**, etc.

## Managing content-aware search groups

Content-aware search groups provide the ability to search for log records and other data objects by various features of data, such as file types, keywords, document properties, etc. Search groups are similar to content groups employed by content-aware rules in the DeviceLock Service and content discovery rules in the Discovery Server. Like content groups, search groups are used to determine the data to find. A query that includes a search group returns results matching that group.

Search groups are administered and stored separately from search queries. This provides for centralized management of search groups with the ability to reuse them in different queries and tasks. When administering search groups, bear in mind that changing a search group affects the search results of all queries and tasks based on that group.

Search groups are stored in the DeviceLock Content Security Server's database on the designated SQL Server. In the DeviceLock Management Console, the repository of these groups is referred to as the Content Database. Since search groups are stored on the SQL Server, the Content Database can be independent of the DeviceLock console host and optionally the DeviceLock server host used to manage the database/s on the SQL Server.

Search groups can be added to full-text search queries (see [Steps to perform a search](#)) as well as to search task queries ( [Setting up the search query](#)).

The following sections provide instructions for managing search groups, as well as a description of search groups and their settings by group type:

- [Dialog box for managing search groups](#) - Select, view, create, and configure content-aware search groups.
- [File Type Detection groups](#) - Search for files by the value of their File Type field.
- [Keywords groups](#) - Search for specific keywords or phrases in data/files.
- [Pattern groups](#) - Search for specific text fragments by using regular expressions.
- [Document Properties groups](#) - Search for specific document properties, such as size, name, etc.
- [Complex groups](#) - Compose a logical expression of multiple group types.

## Dialog box for managing search groups

The dialog box for managing search groups appears when selecting the **Content-Aware Group** command from the **Insert** menu in the **Search** box on the search page (see [Steps to perform a search](#)), or when clicking the **Content Database** button next to the **Query** field on the page for configuring a search task's query (see [Setting up the search query](#)).

The dialog box lists the groups from the server's Content Database. For each group, the list displays the name and type of the group along with the **Indexable** check box. The list can be filtered by selecting the desired group type in the **Show** field under the list. The list holds only the groups of the type selected in the **Show** field.

The **Indexable** check box affects only Pattern groups and Complex groups that include Pattern groups. For other group types, it is always selected and cannot be cleared. Selecting this check box for a particular Pattern/Complex group causes the search index to include additional information in order to provide that group with the following advanced search capabilities:

- Regular expressions to search for text fragments consisting of multiple words and/or groups of digits separated by spaces or punctuation marks. Without the **Indexable** check mark, the Pattern group is only capable to search for a single word or sequence of digits.
- The **Validation**, **Case sensitive**, **Visual anti-spoofing**, and **Cyrillic transliteration** search options (for option descriptions, see [Setting up, viewing or changing a Pattern group](#)). Without the **Indexable** check mark, these options have no effect.
- The characters ^ and \$ to match the beginning and end of a line. Without the **Indexable** check mark, the search index does not contain information about line feeds, so expressions containing the beginning-of-line character (^) and/or end-of-line character (\$) will not work.

After selecting the **Indexable** check box, the advanced search capabilities are available only on newly indexed data. To extend them to previously indexed data, a new search index must be created. Follow the instruction in [Rebuilding the index on demand](#), and click **Yes** in the confirmation message box to create a new search index in place of the existing one (this can take a long time).

---

### Important

- Selecting the **Indexable** check box may increase the time required to build the search index by several times.
  - For groups that do not require advanced search capabilities, the **Indexable** check box is selected by default and cannot be cleared. This does not affect the index build time.
  - The advanced search capabilities do not extend to previously indexed data that is not on the server at the time of creating a new search index after selecting the **Indexable** check box (for example, documents deleted from the Shadow Log).
- 

In the dialog box for managing search groups, one can perform the following tasks:

- Add one or more groups to the search query. Select the desired group/s in the list and click **Add**, or double-click the desired group.
- Create a new group or view/change settings of an existing group:

- To create a new group using the default settings, click the arrow next to the **Add Group** button and select the desired type of group.
- To create a new group using the settings of another already existing group, select this group in the list and click the **Duplicate** button.

---

**Note**

Duplication is frequently used to create editable copies of built-in groups.

---

- To view or change the settings of an existing group, select that group in the list and click the **Edit Group** button (for groups created by an administrator) or the **View Group** button (for built-in groups, which are not allowed to change).

As a result, a dialog box appears to set, view, or change group settings.

- Delete a group that was created earlier by an administrator. Select the group in the list and click the **Delete Group** button. For built-in groups, this button is unavailable, as DeviceLock does not allow deleting its built-in groups.

When creating, duplicating, viewing, or editing a group, the console employs a unified dialog box for managing the settings of groups of the given type. These settings per group type are described in the following sections:

- [File Type Detection groups](#)
- [Keywords groups](#)
- [Pattern groups](#)
- [Document Properties groups](#)
- [Complex groups](#)

## File Type Detection groups

File Type Detection groups are used to find files of specific verified type, regardless of how the file might be named or what file name extension it might have. For example, with such a group, one could find shadow copies of files of specified types. A group can be configured to specify one or more file types. The search is then performed by the value of the “File Type” field assigned to files in the DeviceLock logs. The server returns the files for which the value of this field matches any of the types specified in the group.

The Search Server provides a wide range of predefined (built-in) File Type Detection groups.

Administrators can use built-in groups as they are, create editable copies (duplicates) of built-in groups, or create new, custom groups to suit a particular organization’s needs. Built-in groups make it easy to configure search requests without necessarily having to define custom groups. Review [a list of built-in File Type Detection groups](#) for further details.

For built-in groups of this type, one can only view their file types in the dialog box described in the section that follows. Changing built-in groups is not allowed. To change the file type members of a built-in group, create an editable copy of it by duplicating the group (see [Dialog box for managing search groups](#)).

### ***Setting up, viewing or changing a File Type Detection group***

When creating, duplicating, viewing, or editing a File Type Detection group (see [Dialog box for managing search groups](#)), the console employs a dialog box composed of two panes:

- **Content Group** - The left pane under this title lists the file types included in the given group. For each type, it displays possible file name extensions and a brief description of that type. The group serves to find files of the type/s listed here. During a search, the file types are combined by OR logic, i.e. a file matches this group if the file's type matches any one listed. The **Name** field above the list of types is used to set, view, or change the name of the group.
- **Available Content** - The right pane under this title displays a list from which file types can be selected to include in the group. For each type, it displays possible file name extensions and a brief description of that type.

---

#### Note

This pane is not displayed when viewing a File Type Detection group.



---



The field above the **Available Content** list is used to search for the desired type/s. Enter a search string in this field and then search or filter by that string:



- Click the **Find** or **Find Previous** button to search for file name extensions or file type descriptions in which the given string occurs.  
Click **Find** to go to the next occurrence of the search string in the list. Click **Find Previous** to go back to the previous occurrence of that string.
- Click the **Filter** button to list only those file types that have the given search string in the file name extension or file type description.



The search string field allows the use of an asterisk (\*) to represent an arbitrary sequence of characters and the use of a question mark (?) to represent any single character.

The buttons between the dialog box panes are used to add or remove file types from the group:

 - Select file types in the right pane and click  to add them to the group. The selected file types are added to the list in the left pane.

 - Select file types in the left pane and click  to remove them from the group. The selected file types are removed from the list in the left pane.

 - Click this button to remove all file types from the group. Clicking  clears the list in the left pane.

 - Click this button to add all available file types to the group. Clicking  adds all file types listed in the right pane to the list in the left pane.

---

#### Note

These buttons are not displayed when viewing a File Type Detection group.

---

## Keywords groups

Keywords groups enable the server to find log records and data objects (such as files, e-mails, or instant messages) by specific words and/or phrases, referred to as "keywords". For example, by

using groups of this type, one could find entries of shadow files/logs and audit logs in which specific keywords are encountered. A group can be configured to specify the desired keywords and search settings (for example, whether to search for all keywords or at least one of them). Then the server can search for objects containing the keywords specified in that group.

The Search Server provides a wide range of predefined (built-in) Keywords groups. Administrators can use built-in groups as they are, create editable copies (duplicates) of built-in groups, or create new custom groups to suit a particular organization's needs. Built-in groups make it easy to configure search requests without necessarily having to define custom groups. Review [a list of built-in Keywords groups](#) for further details.

For built-in groups of this type, one can only view their keywords and other settings in the dialog box described in the section that follows. Changing built-in groups is not allowed. To change the keywords in a built-in group, create an editable copy of it by duplicating the group (see [Dialog box for managing search groups](#)).

### ***Setting up, viewing or changing a Keywords group***

When creating, duplicating, viewing, or editing a Keywords group (see [Dialog box for managing search groups](#)), the console employs a dialog box with the following group setting control fields:

- **Name, Description** - Set, view, or change the name and description of the group.
- **Condition** - View or select the search condition:
  - **Match any keyword(s)** - The group searches for objects that contain at least one of its keywords.
  - **Match all keyword(s)** - The group searches for objects that contain each of its keywords.
- **Keywords** - View or change the group's keywords:
  - To add a keyword, click the **Add** button beneath the keyword list, and then type the desired word or phrase. When finished, press Enter.
  - To change a keyword already in the list, double-click in the **Keywords** field of the respective list entry, and type the desired changes. When finished, press Enter.
  - To remove keywords, select them in the list and click the **Delete** button beneath the keyword list.
  - To add keywords from a text file, click the **Load** button beneath the keyword list and open the file in the dialog box that appears. Each keyword in this file must be on a separate line, with a line break after the last character of the keyword.

In the keyword list, one can view or change the following search option individually for each keyword:

- **Whole Word** - Determines whether to search for only those objects in which the keyword occurs as a separate word rather than a part of another word. When the **Whole Word** check box is selected, the server looks for a word that exactly matches the given keyword (for example, searching for the keyword `test` will not find the word `contest` or `testimony`). When this check box is cleared, the server also looks for words that contain the given keyword (`contest` and `testimony` will then appear in the search results along with the keyword `test`).



## Pattern groups

Pattern groups enable the server to find log records and data objects (such as files, e-mails, or instant messages) by matching their text content to regular expressions, referred to as “patterns”. Regular expressions provide a way to search for complex combinations of characters like credit card numbers, social security numbers, e-mail addresses or phone numbers. Pattern groups employ Perl regular expressions, described at [perldoc.perl.org/perlrequick.html](http://perldoc.perl.org/perlrequick.html) and [perldoc.perl.org/perlretut.html](http://perldoc.perl.org/perlretut.html).

By using Pattern groups, one could find, for example, shadow copies containing character strings that match specific regular expressions. Such a group can be configured to specify the desired regular expression/s and other search settings (see [Setting up, viewing or changing a Pattern group](#)). Then the server can search for objects that match the regular expression/s from that group.

Search Server provides a wide selection of predefined (built-in) Pattern groups. Administrators can use built-in groups as they are, create editable copies (duplicates) of built-in groups, or create new, custom groups to suit a particular organization’s needs. Built-in groups make it easy to configure search requests without necessarily having to define custom groups. Review [a list of built-in Pattern groups](#) for further details.

For built-in groups of this type, one can only view their regular expressions and other settings in the dialog box described in the section that follows. Changing built-in groups is not allowed. To change the pattern logic of a built-in group, create an editable copy of it by duplicating the group (see [Dialog box for managing search groups](#)).

### ***Setting up, viewing or changing a Pattern group***

When creating, duplicating, viewing, or editing a Pattern group (see [Dialog box for managing search groups](#)), the console employs a dialog box with the following group setting control fields:

- **Name, Description** - Set, view, or change the name and description of the group.
- **Expression** - View, add, or change the regular expression/s for this group. One or more expressions can be entered by typing in the **Expression** field, with just one expression per line. For details on regular expressions, refer to the tutorials at [perldoc.perl.org/perlrequick.html](http://perldoc.perl.org/perlrequick.html) and [perldoc.perl.org/perlretut.html](http://perldoc.perl.org/perlretut.html).

When matching a data object to the group during a search, the server counts the total number of data matches with the expression/s specified in this field, and concludes whether the object matches the group depending upon the search condition selected.

- **Validate** - Check the regular expression syntax.
- **Validation** - When configured to perform validation, the group detects a match only in case of a match to the selected validation type in addition to the regular expression specified. To match the group, data needs to match the expression and additionally pass the validation. If **No validation** is selected in this field, the group does not perform validation. To match the group in this case, data only needs to match the expression specified.

To configure validation, select the desired type from the [drop-down list in this field](#).



- **Case sensitive** - When this check box is selected, the group distinguishes between lowercase and uppercase characters. For example, the words `Term` and `term` in this case are considered different words, so the group can match the word `Term` but not `term`.  
When this check box is cleared, the group does not distinguish between uppercase and lowercase characters. In this case, if `Term` matches such a group, then `term` or even `tErM` will match that group as well.
- **Visual anti-spoofing** - When this check box is selected, the group identifies data matching its regular expression even if certain data characters are replaced with other ones similar in appearance or meaning, including:
  - Latin characters in the Russian text (such as Latin `b` in place of Russian `ь`)
  - Latin characters in place of certain numerals (such as Latin `S` in place of digit `5`)
  - Russian characters in the English text (such as Russian `п` in place of Latin `n`)
  - Russian characters in place of certain numerals (such as Russian `3` in place of digit `3`)
  - Certain symbols in place of Russian characters (such as `*` (asterisk) in place of Russian `ж`)
  - Numerals in place of certain Latin or Russian characters (such as digit `1` in place of Latin `I` or digit `4` in place of Russian `ч`)
  - Arabic-Indic (Eastern Arabic) numerals in place of normal Arabic numerals (such as symbol `٣` in place of digit `3` or symbol `٨` in place of digit `8`)
 When this check box is cleared, the group strictly distinguishes characters regardless of whether or not they are similar in appearance or meaning.
- **Cyrillic transliteration** - When this check box is selected, the group recognizes Cyrillic text to be detected regardless of whether the text is written in Cyrillic or Latin letters. For example, if the Russian word `Серия` matches the group, then the word `Seriya` will match it as well.  
When this check box is cleared, the match of the text to the group strictly depends upon the alphabet used to spell the text. For example, the group can match the word `Серия` but not `Seriya`.
- **Advanced** - Test the regular expression on sample data. Click **Advanced** to display or hide the **Test sample** box.
- **Test sample** - Enter a test string to test and view the results. Test results are highlighted in real time. All matches to the group's regular expression are displayed in green, and the character sequences not matching that expression are displayed in red.

---

## Important

- To provide a Pattern group with advanced search capabilities, it is necessary to select the **Indexable** check box for that group in the [Dialog box for managing search groups](#). Otherwise, the group is only capable to search for a single word or sequence of digits, and the following group settings may function incorrectly or not function at all: **Validation; Case sensitive; Visual anti-spoofing; Cyrillic transliteration**.
  - For Pattern groups that do not require advanced search capabilities, the **Indexable** check box is selected by default and cannot be cleared.
  - After upgrading DeviceLock, rebuilding the search index may be required to search for credit card numbers and e-mail addresses in the data indexed by the old DeviceLock version. To rebuild the index, follow the instruction given in [Rebuilding the index on demand](#) and, when prompted, click **Yes** in the confirmation message box to replace the existing index with the new one.
  - You cannot use the built-in **Credit Card Number** Pattern group to find log records and data objects that contain credit card numbers of the MIR payment system. To search for such data, create and use a duplicate of the built-in **Credit Card Number** group.
- 

## Document Properties groups

Document Properties groups enable the server to find data objects (such as documents, e-mails, or instant messages) by various parameters that can be retrieved from DeviceLock logs. All these parameters, referred to as “document properties”, are listed and described in [Setting up, viewing or changing a Document Properties group](#) below. Using a Document Properties group, one could find, for example, shadow copies of documents with particular values of properties such as Title, Subject, Categories, Last saved by, etc. A group can be configured to specify the property values of the documents to find. Then the server can search for documents whose properties match that group.

### ***Setting up, viewing or changing a Document Properties group***

When creating, duplicating, viewing, or editing a Document Properties group (see [Dialog box for managing search groups](#)), the console employs a dialog box with the following group setting control fields:

- **Name, Description** - Set, view, or change the name and description of the group.
- **File name** - Set, view, or change the desired file names. If this parameter is set, the group searches for files with any of the specified names.  
To specify multiple names, separate them by a semicolon (;). In file names, an asterisk (\*) can be used to represent zero or more characters and a question mark (?) can be used to represent any single character.
- **File size** - Set, view or change the desired file size in bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), or terabytes (TB). If this parameter is set, the group searches for files that match the selected size option.  
The following size options are available:
  - **Not specified** (selected by default) - Search for files of any size.
  - **Equal to** - Search for files of exactly the size specified.

- **Less than** - Search for files that are smaller than the size specified.
- **More than** - Search for files that are larger than the size specified.
- **Between** - Search for files of the size in the specified range.

---

### Important

After upgrading DeviceLock, rebuilding the search index may be required to search by file size in the data indexed by the old DeviceLock version. To rebuild the index, follow the instruction given in [Rebuilding the index on demand](#) and, when prompted, click **Yes** in the confirmation message box to replace the existing index with the new one.

---

- **Password protected** - Select this check box to search for shadow copies of protected documents. When this check box is selected, the search returns only documents with the status of "Yes" in the **Protected** field of the respective log record. When this check box is cleared, the search disregards the value in that field.
- **Additional Parameters** - Search using document properties, such as built-in and custom properties of Microsoft Office documents and other document types; classification labels applied by third-party products like Boldon James Classifier; senders and recipients of instant messages and emails; and device types or protocols of the data objects to find.

The following additional parameters are available:

- **Title, Subject, Tags, Company, Manager, Comments, Authors, Categories, Last saved by** - Set, view or change values matching some frequently used properties of documents to search for in the logs. Supported are properties of MS Office documents (.docx, .xlsx, .pptx, .vsdx), .pdf, and compound documents. The title of the field corresponds to the property name specified in document management applications such as MS Office Word or Adobe Acrobat. These fields allow the use of wildcard: an asterisk (\*) can be used to represent zero or more characters and a question mark (?) can be used to represent any single character. Multiple values can be entered in a field by separating them with a semicolon (;). Example of entering two values with wildcards: \*Report\*; \*Account\*.

Values entered in different fields are combined by AND logic. If multiple values are entered in the same field, they are combined by OR logic.

---

### Note

To search for files with arbitrary non-empty value of any of these document properties, use the ?\* mask. An asterisk without a question mark matches any value of the property, as well as no property (empty value).

---

- **Custom & classification fields** - View or enter values matching various built-in or custom properties of documents to search for. Supported are properties of MS Office documents (.docx, .xlsx, .pptx), .pdf and compound documents.  
To enter a single value for some property, use the following syntax:  
<property name>=<property value>. Thus, Division=Sales represents the value of Sales for the Division property. To enter multiple values for the same property, separate them with a comma.

In this case, values are combined by OR logic. Thus, Division=Sales,Finance represents the value of Sales OR Finance for the Division property.

To enter values for multiple properties, separate property entries by a semicolon, such as <name1>=<value11>,<value12>; <name2>=<value21>. Values of different properties are combined by AND logic while different values of the same property are combined by OR logic. Thus, Division=Sales,Finance; Office=Head Office represents the value of Sales OR Finance for the Division property AND the value of Head Office for the Office property.

By using the **Custom & classification fields** box, the group can also be configured to recognize classification labels of third-party products like Boldon James Classifier that save their label values in document properties. If the label is the exact value of some property, then, to recognize it, one can use the syntax described above: <property name>=<property value>. The value of whichever property of the document serves for the designation of the label is determined by the settings of the third-party product.

To set up the group to recognize Boldon James Classifier's SISL labels, a syntax is used that indicates the ID of the uid element of the desired label: uid=<ID value>. The ID value can be found from the XML data of the SISL label stamped on a document classified. For further details, see [Recognizing Boldon James Classifier Labels](#).

In the **Custom & classification fields** box, a semicolon (;) can be used as a separator to enter more than one entry designating document properties and/or classification labels. All semicolon-separated entries are combined by AND logic.

---

#### Note

To assist with configuring the group, the **Custom & classification fields** box stores previous entries and provides them for selection from the drop-down list attached to this box.

---

- **Sender(s)** - Set, view, or change the desired sender identifiers for the following protocols: IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMTP, Telegram, Viber, Web Mail, WhatsApp, Zoom. If this parameter is set, the group searches for records associated with any of the specified sender/s.  
To specify multiple senders, separate sender identifiers by a semicolon (;). In sender identifiers, an asterisk (\*) can be used to represent zero or more characters and a question mark (?) can be used to represent any single character.
- **Recipient(s)** - Set, view or change the desired recipient identifiers for the protocols IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMTP, Telegram, Viber, Web Mail, WhatsApp, Zoom, as well as for the following social networks: Facebook, Google+, LiveJournal, LinkedIn, LiveInternet, Myspace, Odnoklassniki, Twitter, VKontakte. If this parameter is set, the group searches for records associated with any of the specified recipient/s.  
To specify multiple recipients, separate recipient identifiers by a semicolon (;). In recipient identifiers, an asterisk (\*) can be used to represent zero or more characters and a question mark (?) can be used to represent any single character.
- **Source(s)** - View or select the desired device types or protocols from the drop-down list. If this parameter is set, the group searches for records associated with any of the selected device type/s or protocol/s.

When using additional parameters, consider the following:

- Different parameters are combined by AND logic, that is, the group recognizes a document if it matches each of the parameters configured. Thus, for a document to be recognized by a group that has the `Title` and `Subject` parameter values specified, both the `Title` and `Subject` properties of the document must have the respective values. If it is required to combine parameters by OR logic, one could configure a Complex group by adding to it a separate Document Properties group for each parameter.
- It is possible to specify multiple values for the same parameter by separating them with a semicolon. In this case, the values are combined by OR logic, so that the group recognizes a document if it matches any of the values specified. Thus, if `Report; Account` is specified in the `Title` parameter, then the group recognizes documents that have the `Title` property value of `Report OR Account`.

## Complex groups

Complex groups are used to combine search groups by using logical expressions. Search data matches the complex group when it meets the group's condition. A condition is a logical expression that consists of one or more criteria. Each of the criteria leverages a certain search group, and it evaluates to `true` if the search data matches that group; otherwise, it evaluates to `false`. The value of the expression is calculated of the current values of its criteria, and the data is considered to match the complex group when the expression evaluates to `true`.

### *Setting up, viewing, or changing a Complex group*

When creating, duplicating, viewing, or editing a Complex group (see [Dialog box for managing search groups](#)), a dialog box is used to add or remove criteria, combine them by AND/OR logic, and group them with brackets:

- Use the buttons above the list of criteria to add or remove criteria, to view their search groups, and to change the follow order of the criteria in the logical expression:
  - **Add** - Adds a new item to the end of the list of criteria.  
To add an item, click the **Add** button, or double-click a blank area in the list of criteria.
  - **Insert** - Adds a new item before the one selected in the list of criteria.  
To add/insert criteria, the console provides a dialog box where one or more groups can be selected. Then, it adds one or more criteria to the condition, one for each of the selected groups. The name of the group is displayed in the **Criteria** field.
  - **View** - Opens a dialog box to view the settings of the group selected in the list of criteria. This dialog box is similar to the dialog box for configuring groups of the respective type, in which the group settings are read-only.  
To view the settings of the group, click the **View** button, or double-click the group in the list of criteria.
  - **Delete** - Removes the selected item as well as the logical operators and brackets specified along with that item in the list of criteria.

- **^, v** (up and down arrows) - Moves the selected item up and down in the list of criteria.  
Note that moving criteria up and down in the list may break the logical structure of the expression. Click the **Validate** button to check the syntax of the expression and display the resulting expression in the **Result** box.
- Select check boxes in the **NOT** column to reverse the logical value returned by the respective criteria.
- Click in the column titled with a bracket ( **(** or **)** ) to add one or more brackets.  
Brackets serve to avoid ambiguity of multi-criteria expressions. For example, the expression A AND B OR C could mean (A AND B) OR C, or it could mean A AND (B OR C). Use brackets to accurately determine the order and intention in which expressions are calculated.

---

#### Note

When moving an entry to the place of an adjacent one in the criteria list, the **NOT** check box setting moves together with the entry if the number of opening brackets is less than or equal to that of closing ones both in the moved entry and in the entry to which place it is moved. If at least one of them has more opening brackets than closing ones, the **NOT** check box setting does not move to the adjacent entry. Such a solution helps preserve the logical structure of the expression when the order of the list entries changes.

---

- Click in the **AND/OR** column to select the operator to combine the criteria into a logical expression. By default, **AND** is selected, so data objects match the group only if they meet all the specified criteria. Select **OR** for data objects to match the group if they meet at least one of those criteria.
- **Validate** - Checks the syntax of the logical expression, removes unnecessary brackets if any, and displays the resulting expression in the **Result** box.
- **Clear** - Removes all criteria from the group's condition. As a result, the group has no search condition specified.

The dialog box for configuring complex groups also includes the fields to set, view, or change the name and description of the group.

## Working with search results

When performing a full-text search, the server returns a search results page that looks like this:

customer	Search	Options >>
----------	--------	------------

Example: secret confidential, "secret confidential", secret AND confidential, secret OR confidential.

Results 1 - 3 for **customer**.

1. 4:58:54 PM Success Win10PC2 Removable Write E:\Docs\customer 3.pdf 772.05 KB WIN10PC2\Adm in 1772 C:\Windows...  
[Log Parameters](#)  
[Document Parameters](#)  
10/5/2017 4:58:54 PM - 772.05 KB - E:\Docs\customer 3.pdf  
Shadow Log  
[Open](#) - [Save](#) - [View](#)
2. 4:58:53 PM Success Win10PC2 Removable Write E:\Docs\customer 2.pdf 127.37 KB WIN10PC2\Adm in 1772 C:\Windows...  
[Log Parameters](#)  
[Document Parameters](#)  
10/5/2017 4:58:53 PM - 127.37 KB - E:\Docs\customer 2.pdf  
Shadow Log  
[Open](#) - [Save](#) - [View](#)
3. 4:58:53 PM Success Win10PC2 Removable Write E:\Docs\customer 1.pdf 757.39 KB WIN10PC2\Adm in 1772 C:\Windows...  
[Log Parameters](#)  
[Document Parameters](#)  
10/5/2017 4:58:53 PM - 757.39 KB - E:\Docs\customer 1.pdf  
Shadow Log  
[Open](#) - [Save](#) - [View](#)

1

The search results page is divided into the following viewing areas:

- [Search query](#) - Displays the search criteria that were used.
- [Statistics bar](#) - Shows the number of results displayed on the current search results page.
- [Search results](#) - Displays a numbered list of items containing information that matched the search criteria.
- [Results navigator](#) - Shows how many results pages are returned, and allows one to navigate from page to page.

These areas are described in more detail in the sections that follow.

### **Search query**

This area is located at the top of the search results page. Click **Options** to view all the search parameters that were used during the search:

Search

Options <<

Example: secret confidential, "secret confidential", secret AND confidential, secret OR confidential.

Display  results per page

Limit results to the following logs:

- ☒ Audit Log
- ☐ Server Log
- ☒ Shadow Log
- ☐ Monitoring Log
- ☒ Deleted Shadow Data Log
- ☐ Policy Log
- ☐ UAM Log

Limit results to the following date range:

From:

To:

Limit results to the following parameters:

Sender(s):

Recipient(s):

File type(s):

Source(s):

For a description of the search parameters, see [Steps to perform a search](#).

### Statistics bar

This area is located directly above the search results area, and it looks like this:

Results 1 - 3 for **customer**.

### Search results

This area is located below the search query area and statistics bar, and it looks like this:



1. 4:58:54 PM Success Win10PC2 Removable Write E:\Docs\customer 3.pdf 772.05 KB WIN10PC2\Adm in 1772 C:\Windows...  
[Log Parameters](#)  
[Document Parameters](#)  
 10/5/2017 4:58:54 PM - 772.05 KB - E:\Docs\customer 3.pdf  
 Shadow Log  
[Open](#) - [Save](#) - [View](#)
2. 4:58:53 PM Success Win10PC2 Removable Write E:\Docs\customer 2.pdf 127.37 KB WIN10PC2\Adm in 1772 C:\Windows...  
[Log Parameters](#)  
[Document Parameters](#)  
 10/5/2017 4:58:53 PM - 127.37 KB - E:\Docs\customer 2.pdf  
 Shadow Log  
[Open](#) - [Save](#) - [View](#)
3. 4:58:53 PM Success Win10PC2 Removable Write E:\Docs\customer 1.pdf 757.39 KB WIN10PC2\Adm in 1772 C:\Windows...  
[Log Parameters](#)  
[Document Parameters](#)  
 10/5/2017 4:58:53 PM - 757.39 KB - E:\Docs\customer 1.pdf  
 Shadow Log  
[Open](#) - [Save](#) - [View](#)

A search result includes the following items:

- **Snippets** - Text fragments containing query words (highlighted bold). These snippets allow one to see the context in which the query words were found. Only the first three snippets are displayed per search result.
- **Log Parameters** - Summary information found in the log for the search result, depending on the log type. Click the plus sign (+) to expand **Log Parameters** and view this information.

---

#### Note

Empty fields of log records are not displayed in **Log Parameters**.

---

For search results retrieved from the Audit Log, the **Log Parameters** information includes:

- **Type** - The class of the event: **Success** - an allowed action; **Failure** - a denied action; **Information** - a content detection event; **Warning** - indication of a potential problem. Matches the **Type** column data in the server Audit Log Viewer.
- **Computer** - The name of the computer on which the event occurred. Matches the **Computer** column data in the server Audit Log Viewer.
- **Date/Time** - The date and time that the DeviceLock Service logged the event. Matches the **Date/Time** column data in the server Audit Log Viewer.
- **Source** - The type of device or protocol that caused the event. Matches the **Source** column data in the server Audit Log Viewer.
- **Action** - The user's activity type. Matches the **Action** column data in the server Audit Log Viewer.
- **Name** - The name of the object (file, USB device, etc.) associated with the event. Matches the **Name** column data in the server Audit Log Viewer.

- **Information** - Other device- or protocol-specific information for the event, such as the access flags, the device or protocol name, device ID and description, etc. Matches the **Information** column data in the server Audit Log Viewer.
- **Reason** - The cause of the event. Matches the **Reason** column data in the server Audit Log Viewer.
- **User** - The name of the user associated with the event. Matches the **User** column data in the server Audit Log Viewer.
- **PID** - The identifier of the process associated with the event. Matches the **PID** column data in the server Audit Log Viewer.
- **Process** - The fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path. Matches the **Process** column data in the server Audit Log Viewer.
- **Event** - The number identifying the event type. Matches the **Event** column data in the server Audit Log Viewer.
- **Received Date/Time** - The date and time that the DeviceLock Enterprise Server received the event. Matches the **Received Date/Time** column data in the server Audit Log Viewer.
- **Server** - The name of the DeviceLock Enterprise Server host that received the event from the DeviceLock Service. Matches the **Server** column data in the server Audit Log Viewer.
- **Consolidation Server** - The name of the remote server from which the event was last received during log consolidation. Matches the **Consolidation Server** column data in the server Audit Log Viewer.
- **Consolidated Date/Time** - The date and time that the event was last received from the remote server during log consolidation. Matches the **Consolidated Date/Time** column data in the server Audit Log Viewer.
- **DeviceLock Enterprise Server** - The name of the DeviceLock Enterprise Server host from which the Search Server indexed the event data.

For search results retrieved from the Shadow Log or Deleted Shadow Data Log, the **Log Parameters** information includes:

- **Status** - The status of the record: **Success** - shadow copy successfully logged; **Incomplete** - shadow copy possibly not completely logged; **Failed** - shadow copy of data the transmission of which was blocked by Content-Aware Rules. Matches the **Status** column data in the server Shadow Log Viewer.
- **Computer** - The name of the computer on which the shadow copy was received. Matches the **Computer** column data in the server Shadow Log Viewer.
- **Date/Time** - The date and time that the shadow copy was logged by the DeviceLock Service. Matches the **Date/Time** column data in the server Shadow Log Viewer.
- **Source** - The type of the device or protocol involved. Matches the **Source** column data in the server Shadow Log Viewer.
- **Action** - The user's activity type. Matches the **Action** column data in the server Shadow Log Viewer.

- **File Name** - The original path to the file or the auto-generated name of the data that originally was not a file (such as CD/DVD/BD images, data written directly to the media, or transferred through the serial/parallel ports). Matches the **File Name** column data in the server Shadow Log Viewer.
- **File Size** - The size of the data. Matches the **File Size** column data in the server Shadow Log Viewer.
- **File Type** - The real type of the file. Matches the **File Type** column data in the server Shadow Log Viewer.
- **Reason** - The cause of the event. Matches the **Reason** column data in the server Shadow Log Viewer.
- **Protected** - Indicates the protection status of the file. Matches the **Protected** column data in the server Shadow Log Viewer.
- **Information** - Other device- or protocol-specific information for the event, such as the access flags, the device or protocol name, device ID and description, etc. Matches the **Information** column data in the server Shadow Log Viewer.
- **User** - The name of the user who transferred the data. Matches the **User** column data in the server Shadow Log Viewer.
- **PID** - The identifier of the process used to transfer the data. Matches the **PID** column data in the server Shadow Log Viewer.
- **Process** - The fully qualified path to the process executable file. In some cases, the process name may be displayed instead of the path. Matches the **Process** column data in the server Shadow Log Viewer.
- **Received Date/Time** - The date and time that the DeviceLock Enterprise Server received the event. Matches the **Received Date/Time** column data in the server Shadow Log Viewer.
- **Server** - The name of the DeviceLock Enterprise Server host that received the event from the DeviceLock Service. Matches the **Server** column data in the server Shadow Log Viewer.
- **Consolidation Server** - The name of the remote server from which the event was last received during log consolidation. Matches the **Consolidation Server** column data in the server Shadow Log Viewer.
- **Consolidated Date/Time** - The date and time that the event was last received from the remote server during log consolidation. Matches the **Consolidated Date/Time** column data in the server Shadow Log Viewer.
- **DeviceLock Enterprise Server** - The name of the DeviceLock Enterprise Server host from which the Search Server indexed the event data.

For search results retrieved from the UAM Log, the **Log Parameters** information includes:

- **Computer** - The name of the computer on which the user activity monitoring session was recorded. Matches the **Computer** column data in the server UAM Log Viewer.
- **Date/Time** - The date and time that the recording of the monitoring session started. Matches the **Date/Time** column data in the server UAM Log Viewer.
- **Type** - The types of recording available in this session: **Video** - The computer screen video recording only; **Keylogger** - The computer keystrokes recording only; **Video, Keylogger** - The

computer screen recording and keystrokes recording. Matches the **Type** column data in the server UAM Log Viewer.

- **Rule** - The name of the rule that caused the recording. Multiple rules could be listed here if more than one rule triggered during this recording. Matches the **Rule** column data in the server UAM Log Viewer.
- **Reason** - The triggering criteria of the rule that caused the recording. In case of multiple rules, a separate list of triggering criteria is specified for each rule. Matches the **Reason** column data in the server UAM Log Viewer.
- **Duration** - The time span that recording lasted. Matches the **Duration** column data in the server UAM Log Viewer.
- **User** - The name of the user whose activity is recorded in this session. Matches the **User** column data in the server UAM Log Viewer.
- **Received Date/Time** - The date and time that the DeviceLock Enterprise Server received this session record from the DeviceLock Service. Matches the **Received Date/Time** column data in the server UAM Log Viewer.
- **Server** - The name of the DeviceLock Enterprise Server host that received this session record from the DeviceLock Service. Matches the **Server** column data in the server UAM Log Viewer.
- **Consolidation Server** - The name of the remote server from which this session record was last received during log consolidation. Matches the **Consolidation Server** column data in the server UAM Log Viewer.
- **Consolidated Date/Time** - The date and time that this session record was last received from the remote server during log consolidation. Matches the **Consolidation Date/Time** column data in the server UAM Log Viewer.
- **DeviceLock Enterprise Server** - The name of the DeviceLock Enterprise Server host from which the Search Server indexed the monitoring session data.

For search results retrieved from the Server Log, the **Log Parameters** information includes:

- **Type** - The class of the event: **Success**, **Information**, **Warning**, or **Error**. Matches the **Type** column data in the Server Log Viewer.
- **Date/Time** - The date and time when the event occurred. Matches the **Date/Time** column data in the Server Log Viewer.
- **Event** - The number identifying the event type. Matches the **Event** column data in the Server Log Viewer.
- **Information** - Event-specific information, such as error/warning descriptions, names and values of changed parameters, etc. Matches the **Information** column data in the Server Log Viewer.
- **Server** - The name of the DeviceLock Enterprise Server host on which the event occurred. Matches the **Server** column data in the Server Log Viewer.
- **Record N** - The record number. Matches the **Record N** column data in the Server Log Viewer.
- **Consolidation Server** - The name of the remote server from which the event was last received during log consolidation. Matches the **Consolidation Server** column data in the Server Log Viewer.

- **Consolidated Date/Time** - The date and time that the event was last received from the remote server during log consolidation. Matches the **Consolidated Date/Time** column data in the Server Viewer.
- **DeviceLock Enterprise Server** - The name of the DeviceLock Enterprise Server host from which the Search Server indexed the event data.

For search results retrieved from the Monitoring Log, the **Log Parameters** information includes:

- **Type** - The class of the event: **Success**, **Information**, **Warning**, or **Error**. Matches the **Type** column data in the Monitoring Log Viewer.
- **Date/Time** - The date and time when the event occurred. Matches the **Date/Time** column data in the Monitoring Log Viewer.
- **Event** - The number identifying the event type. Matches the **Event** column data in the Monitoring Log Viewer.
- **Task Name** - The name of the monitoring task associated with the event. Can be empty if the event does not apply to a monitoring task. Matches the **Task Name** column data in the Monitoring Log Viewer.
- **Computer Name** - The name of the computer belonging to the monitoring task associated with the event. Can be empty if the event does not apply to a computer. Matches the **Computer Name** column data in the Monitoring Log Viewer.
- **Information** - Event-specific information, such as status, error, warning, etc. Matches the **Information** column data in the Monitoring Log Viewer.
- **Server** - The name of the DeviceLock Enterprise Server host on which the event occurred. Matches the **Server** column data in the Monitoring Log Viewer.
- **Record N** - The record number. Matches the **Record N** column data in the Monitoring Log Viewer.
- **Consolidation Server** - The name of the remote server from which the event was last received during log consolidation. Matches the **Consolidation Server** column data in the Monitoring Log Viewer.
- **Consolidated Date/Time** - The date and time that the event was last received from the remote server during log consolidation. Matches the **Consolidated Date/Time** column data in the Monitoring Viewer.
- **DeviceLock Enterprise Server** - The name of the DeviceLock Enterprise Server host from which the Search Server indexed the event data.

For search results retrieved from the Policy Log, the **Log Parameters** information includes:

- **Type** - The class of the event: **Success**, **Information**, **Warning**, or **Error**. Matches the **Type** column data in the Policy Log Viewer.
- **Date/Time** - The date and time when the event occurred. Matches the **Date/Time** column data in the Policy Log Viewer.
- **Event** - The number identifying the event type. Matches the **Event** column data in the Policy Log Viewer.

- **Policy Object** - The name of the policy object associated with the event. Can be empty if the event does not apply to a policy object. Matches the **Policy Object** column data in the Policy Log Viewer.
- **Computer Name** - The name of the computer that caused the event. Can be empty if the event does not apply to a computer. Matches the **Computer Name** column data in the Policy Log Viewer.
- **Information** - Event-specific information, such as status, error, warning, etc. Matches the **Information** column data in the Policy Log Viewer.
- **Server** - The name of the DeviceLock Enterprise Server host that logged the event. Matches the **Server** column data in the Policy Log Viewer.
- **Record N** - The record number. Matches the **Record N** column data in the Policy Log Viewer.
- **Consolidation Server** - The name of the remote server from which the event was last received during log consolidation. Matches the **Consolidation Server** column data in the Policy Log Viewer.
- **Consolidated Date/Time** - The date and time that the event was last received from the remote server during log consolidation. Matches the **Consolidated Date/Time** column data in the Policy Log Viewer.
- **DeviceLock Enterprise Server** - The name of the DeviceLock Enterprise Server host from which the Search Server indexed the event data.
- **Document Parameters** - Summary information retrieved from the document properties for search results from shadow logs Click the plus sign (+) to expand **Document Parameters** and view this information. This information varies depending upon the file type. For example, the following information is displayed in **Document Parameters** for a shadow copy of a Word document:
  - Application - Microsoft Office Word.
  - Author - The name of the user who created the document.
  - Created - The date and time when the document was created.
  - LastSaved - The date and time when the document was last saved.
  - LastSavedBy - The name of the user who last saved the document.
  - RevisionNumber - The number of times the changes to the document were saved.
  - Template - The name of the template attached to the document.
  - Title - The name of the document.
  - TotalEditingTime - The number of minutes that the document has been opened for making changes since it was created.

For search results from the UAM Log, the **Document Parameters** area lists user-entered logins and passwords (if they were logged). The parameter name in this case is Passwords.

- The date and time of the log record.
- The size of the log record. This value is displayed only for shadow copies retrieved from shadow logs.
- The name of the log in which matches of the query occurred.

- **Open, Save, View** - On search results from the shadow logs, these links allow you to open, view, and save shadow copies. For details, see [Working with shadow copies](#).  
On search results from the UAM Log, you can use these links to open, view, or save the recorded keyboard input (keylog). These links only appear on search results that contain a keylog. The keylog opens in the application that is registered to work with HTML files in the operating system. When viewing, the keylog is displayed in a console window. When saving, the keylog is stored as an HTML file.

---

**Note**

If the search produced no results, the search results page displays a message indicating that no matches were found.

---

**Results navigator**

This area is located at the bottom of the search results page, and it looks like this:

[Previous](#) [1](#) [2](#) **[3](#)** [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

To move forward or backward through search results, click **Next** or **Previous**, or click the page number.

## Working with shadow copies

In the DeviceLock console, you can perform the following on search results from shadow logs:

- [Opening a shadow copy](#)
- [Saving a shadow copy](#)
- [Opening and saving a shadow copy in the built-in viewer](#)

**Opening a shadow copy**

Click **Open** under the desired search result.

A shadow copy of the file opens in an application configured for this file type on the computer running the DeviceLock console. If no such application is available, the Open With dialog box appears to select the application with which to open the file. Shadow copies of files from Parallel Port devices open in the DeviceLock Printer Viewer.

The DeviceLock Printer Viewer can display shadow copy of printed documents in the PostScript and native print spooler format, send it to the printer again, or save it as a graphics file (such as BMP, GIF, JPEG, PNG, EMF or TIFF). The following print spooler formats are supported: PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, GDI printing (ZjStream) and EMF Spooled Files.

**Saving a shadow copy**

Click **Save** under the desired search result. Then, in the dialog box that appears, choose the folder and specify the name of the file to hold the copy.

Files sent or received by users are saved in the Shadow Log and can be saved from the log to a local or network folder.

Data that users burn to CD/DVD/BD discs is stored in the Shadow Log as CUE images - one image per each CD/DVD/BD burned.

CD/DVD/BD images as well as other data that originally was not transferred as files (direct media access or serial/parallel ports transfer), have auto-generated names based on the action type, drive letter or device name, and date/time (such as `direct_write(E_) 19_18_29 17_07_2006.bin`).

Each CD/DVD/BD image is composed of two files: a .bin data file (such as `direct_write(E_) 19_18_29 17_07_2006.bin`) and the .cue sheet file with the same name as its data file (such as `direct_write(E_) 19_18_29 17_07_2006_bin.cue`). These two files can be used to mount the CD/DVD/BD image in applications that support the CUE format, such as Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO and many others.

### ***Opening and saving a shadow copy in the built-in viewer***

Click **View** under the desired search result. Then, in the application window that opens, choose from the following view options:

- **Hex** - Displays data in hex as well as in words.
- **Autodetect Text** - Enables the auto-detection of encoding for text and displays data in textual format only.
- **ANSI Text** - Specifies ANSI encoding for text and displays data in textual format only.
- **UTF-16 Text** - Specifies Unicode UTF-16 encoding for text and displays data in textual format only.
- **UTF-16BE Text** - Specifies Unicode UTF-16 (Big Endian) encoding for text and displays data in textual format only.

To save a copy the file, click **Save** in the built-in viewer. Then, in the dialog box that appears, choose the folder and specify the name of the file to hold the copy.

## Automating search operations

The Search Server provides the option to save search queries as tasks and then run them on a schedule or by hand. When running a search task, the server saves the search results in a report that one can view in the console. The server can automatically send reports with search results to e-mail addresses of choice (this option requires a mail server as described in [Specifying mail server for Search Server reports](#)).

When running a search task, the server performs the following actions:

1. Perform a search based on the search query settings.
2. Create a report with information about the task execution that includes search results.
3. Send the report to the e-mail recipients, if specified.

All tasks and their reports are displayed in the console tree under **DeviceLock Content Security Server > Search Server > Tasks**.



Search automation management involves the activities listed in the following table. More details can be found in the topics that follow.

Activity	Details
Create a task	<p>To create a search task:</p> <ul style="list-style-type: none"> <li>In the console tree, expand <b>DeviceLock Content Security Server &gt; Search Server</b>, right-click <b>Tasks</b>, click <b>Create Task</b>, and then specify task settings in the dialog boxes that appear.</li> </ul> <p>For details, see <a href="#">Creating and configuring a new search task</a>.</p>
View a list of tasks	<p>To view a list of search tasks:</p> <ul style="list-style-type: none"> <li>In the console tree, select <b>DeviceLock Content Security Server &gt; Search Server &gt; Tasks</b>.</li> </ul> <p>For details, see <a href="#">Managing existing tasks</a>.</p>
Manage a task	<p>To manage a particular search task:</p> <ul style="list-style-type: none"> <li>In the list of tasks, right-click the task, and use commands from the shortcut menu that appears.</li> </ul> <p>For details, see <a href="#">Managing existing tasks</a>.</p>
View a list of reports	<p>To view a list of reports for a particular search task:</p> <ul style="list-style-type: none"> <li>In the console tree, expand <b>DeviceLock Content Security Server &gt; Search Server &gt; Tasks</b>, and then select the search task under the <b>Tasks</b> node.</li> </ul> <p>For details, see <a href="#">Managing a task and its reports</a>.</p>
Manage reports	<p>To manage a report for a particular search task:</p> <ul style="list-style-type: none"> <li>In the list of reports for that task, right-click the report, and use commands from the shortcut menu that appears.</li> </ul> <p>For details, see <a href="#">Managing a task and its reports</a>.</p>
View a report	<p>To view a report for a particular search task:</p> <ul style="list-style-type: none"> <li>Select the report in the console tree under the node representing that task, or choose <b>Open</b> on the report's shortcut menu.</li> </ul> <p>For details, see <a href="#">Viewing a task's report</a></p>
View the tasks log	<p>The tasks log provides information about events such as task creation, modification, and deletion; search start and finish (including the number of search results); and any errors that occur during task management or execution. To view the list of events:</p> <ul style="list-style-type: none"> <li>In the console tree, select <b>DeviceLock Content Security Server &gt; Search Server &gt; Tasks &gt; Log Viewer</b>.</li> </ul> <p>For details, see <a href="#">Viewing and managing the tasks log</a>.</p>
Manage the tasks	<p>To manage the tasks log:</p>

- log
- In the console tree, select **DeviceLock Content Security Server > Search Server > Tasks > Log Viewer**, right-click in the details pane, and use commands from the shortcut menu that appears.

For details, see [Viewing and managing the tasks log](#).

## Creating and configuring a new search task

Creating a search task involves the following steps:

1. Start the task creation wizard.  
To start the wizard, expand **DeviceLock Content Security Server > Search Server** in the console tree, right-click **Tasks** under **Search Server**, and then click **Create Task**. Alternatively, select **Tasks**, and then click the **Create Task** icon on the toolbar.
2. Set up the search query on the **Query** page of the wizard. For details, see [Setting up the search query](#).  
Setting up a query is similar to configuring a search operation on the **Search Page** (see [Performing a search](#)).
3. Optionally, on the **Schedule** page of the wizard, change the task name, set up a schedule, and specify whether to deliver task reports via e-mail. For details, see [Setting up the search schedule and results settings](#).

### Setting up the search query

On the first page of the task configuration wizard, one can set, view, or change the settings that determine which log records and data objects the task will look for:

- **Query** - One or more strings that determine the words or phrases to find. By default, the strings are combined by AND logic, that is, the search returns the items that match each of the strings specified.

Search groups and saved queries can be added to the **Query** box as follows:

- To add search groups, click the **Content Database** button. Then, in the dialog box that appears, double-click the desired group, or select group/s to add and click the **Add** button. For more information on search groups, see [Managing content-aware search groups](#).  
In the **Query** box, a search group is presented by its name enclosed in percent signs: %group\_name%. It is possible to add a search group by typing a percent sign followed by the group name. As you type, a list of groups that match the entered name appears in the **Query** box, allowing you to select the desired group from that list.
- To add a previously saved query, click the **Saved Query** button. Then, in the dialog box that appears, double-click the desired saved query, or select it and click **OK**. For more information on saved queries, see [Managing saved queries](#).

When composing a query string, one can use commands from the shortcut menu that appears upon a right-click in the **Query** box:

- **Insert** - Displays commands to add a logical operator to the query string. Operators such as AND/OR can be added by typing them in uppercase, or by choosing an operator from the **Insert**

menu. For details, see [About logical operators](#).

To display commands for adding logical operators, one could also press Ctrl+D after clicking in the **Query** box.

- **Save as** - Saves the current query strings for future reuse. For more information, see [Managing saved queries](#).

The shortcut menu in the **Query** box also provides the standard commands for working with text, such as **Cut**, **Copy**, **Paste**, etc.

- **Display <number> results per page** - The number of search results to be included on the task's report page.
- **Limit results to the following logs** - Check boxes to specify the logs to search. One can select any combination of these logs:
  - Audit Log (selected by default)
  - Shadow Log (selected by default)
  - Deleted Shadow Data Log (selected by default)
  - UAM Log
  - Server Log
  - Monitoring Log
  - Policy Log
- **Limit results to the following date range** - Options to search for only the log records in a certain date range:
  - **From** - One can choose the range beginning from the earliest record date in the log (option **First Record**), or select a certain date (option **Records On**). In the latter case, the search is performed on records made no earlier than the selected date.
  - **To** - Together with the **From** setting, one can set the range end to the latest record date in the log (option **Last Record**), or select a certain date (option **Records On**). In the latter case, the search is performed on records made no later than the selected date.
  - **Last** - If selecting this option instead of **From**, one can configure the search to include only the records for a certain number of past days, weeks, or months before the date that the search is performed. Select the desired number and time unit (days, weeks, or months).
- **Limit results to the following parameters** - Options to search for only the items that match the following settings:
  - **Sender(s)** - Sender identifiers for the following protocols: IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMTP, Telegram, Viber, Web Mail, WhatsApp, Zoom. The search returns the results associated with the specified sender/s.  
To specify multiple senders, separate their identifiers by a semicolon (;). Identifiers may include wildcards such as an asterisk (\*) to denote any sequence of zero or more characters and a question mark (?) to denote any single character.
  - **Recipient(s)** - Recipient identifiers for the protocols IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Agent, MAPI, Skype, SMTP, Telegram, Viber, Web Mail, WhatsApp, Zoom, as well as for the following social networks: Facebook, Google+, LiveJournal, LinkedIn, LiveInternet, Myspace,

Odnoklassniki, Twitter, VKontakte. The search returns the results associated with the specified recipient/s.

To specify multiple recipients, separate their identifiers by a semicolon (;). Identifiers may include wildcards such as an asterisk (\*) to denote any sequence of zero or more characters and a question mark (?) to denote any single character.

- **File Type(s)** - File type description (either full or partial), such as "Zip 1.0", "E-Mail message (Var.2)", "Disk Image (Macintosh)". The search returns the results associated with any of the specified file types.

To specify multiple file types, separate file type descriptions by a semicolon (;). Descriptions may include wildcards such as an asterisk (\*) to denote any sequence of zero or more characters and a question mark (?) to denote any single character.

- **Source(s)** - Select device type/s or protocol/s from the drop-down list. The search returns the results associated with any of the selected device type/s or protocol/s.
- **Show only new results** - If this check box is cleared, search results always include all items that match the search query. Select this check box to exclude from search results the items found during the previous runs of the task. When this check box is selected, the task reports behave as follows:
  - The first report after creating the task or changing the task's search query includes all items found.
  - Each subsequent report includes only those items found that were not included in any of the preceding reports.

---

### Important

For an existing task, if one changes the search query or any of the settings listed above, the first report after the change always includes all items found, regardless of whether or not the **Show only new results** check box is selected.

---

## Setting up the search schedule and results settings

On the second page of the task configuration wizard, one can set, view, or change the settings that determine how often the server will run the task, how many search results the task's reports will include, and whether to send search results via e-mail. This page provides the following settings:

- **Task Name** - View the name of the task and change the name as needed. The name cannot be blank or consist solely of spaces, and the name must be unique on the server.
- **Active** - When this check box is selected, the server runs the task according to a schedule.
- **Schedule** - Options to configure a schedule:
  - **One time** - Choose the date and time to run the task, or select the **Now** check box to run the task right after it has been created or modified. The task will run only one time.
  - **Hourly** - Choose the recurrence interval for the task and the date and time to run the task. For example, an interval of 1 produces an hourly schedule and an interval of 2 produces an every-other-hour schedule. The task will run each hour.

- **Daily** - Choose the recurrence interval for the task and the date and time to run the task. For example, an interval of 1 produces a daily schedule and an interval of 2 produces an every-other-day schedule. The task will run at the specified time each day.
- **Weekly** - Choose the recurrence interval for the task, the date and time to run the task, and the days of the week on which to run the task. For example, an interval of 1 produces a weekly schedule and an interval of 2 produces an every-other-week schedule. The task will run at the specified time on each of the specified days.
- **Monthly** - Choose the months in which to run the task and the weeks of the month and the days of the week for each month in which to run the task. The task can also be configured to run on a certain last day of each month.
- **Results** - Options that determine how many results to include in the task's report and whether to deliver reports via e-mail:
  - **Limit to <number> results** - If this check box is cleared, the report may contain a large number of results that could cause a depletion of server resources. Select this check box to limit the number of results the report may contain.
  - **Send results via e-mail** - For the server to deliver the task's reports via e-mail after every run of the task, select this check box and specify the e-mail addresses of the report recipients. One can specify multiple addresses separated by a semicolon (;).  
This option requires a mail server (see [Specifying mail server for Search Server reports](#)). If a mail server is not specified, this option is unavailable.
  - **Do not send results if nothing found** - When selected, this check box prevents the server from sending report e-mails that contain no search results.

## Managing existing tasks

The details pane lists the search tasks stored on the server when **DeviceLock Content Security Server > Search Server > Tasks** is selected in the console tree. The list provides the following details on each task:

- **Name** - The name of the task.
- **Status** - One of the following:
  - **Waiting** - Schedule is inactive, task can be run by hand.
  - **Scheduled** - Waiting for the run on a schedule.
  - **Running** - Task execution is in progress.
  - **Finished** - Last run completed successfully.
  - **Failed** - Task encountered an error.
- **Schedule** - Identifies the task schedule.
- **Results Found** - Total number of items found during all runs of the task, along with the number of items found during the last run enclosed in parenthesis.
- **Results Sent To** - Report recipient addresses if report delivery via e-mail is configured; otherwise, empty.
- **Last Run Time** - Date and time of the last run of this task.

The shortcut menu on the **Tasks** node provides the following commands:

- **Create Task** - Creates a new task. One can specify the desired task settings on the pages that appear upon selecting this command. See [Creating and configuring a new search task](#) for details.
- **Export All Tasks** - Saves all tasks to an export file.
- **Import Tasks** - Imports search tasks from an export file.  
One can export search tasks to a file and then import them from the export file. This function is useful, for example, when copying tasks to another server. See [Exporting and importing tasks](#) for details.
- **Refresh** - Updates the list of tasks with the latest information.

The shortcut menu on a search task in the details pane provides the following commands:

- **Edit Task** - Opens the dialog box to view or change the settings of the selected task.
- **Duplicate Task** - Creates a new task with the settings copied from the selected task. One can view or change the settings of the new task in the dialog boxes displayed by this command. By default, the new task name is composed of the “Copy of” prefix followed by the name of the selected task. When creating two or more copies of a task, the new task name includes a numeric suffix indicating the number of the copy.
- **Delete Task** - Deletes the selected task.  
If a given task was ever run, and thus has any reports, then the console prevents deletion of that task. To delete such a task, one first need to delete the task’s reports.
- **Export Task** - Saves the selected task to an export file.  
One can create a task from an export file by using the **Import Tasks** command on the **Tasks** node in console tree.
- **Run Task** - Use this command to run the task by hand at any time.
- **Stop Task** - Causes immediate stop of the selected task. This command replaces the Run Task command for the tasks that are currently running.
- **Refresh** - Updates the list of tasks with the latest information.

The commands on the shortcut menu can be used to:

- **Run a given task** - Right-click the task, and then click **Run Task**.
- **View or change the search query for a given task** - Right-click the task, click **Edit Task**, and then follow the steps to set up the search query as listed in the [Creating and configuring a new search task](#) section earlier in this document.
- **View or change the name, schedule, or report delivery for a given task** - Right-click the task, click **Edit Task**, and then follow the steps to configure the task name, schedule and results settings as listed in the [Creating and configuring a new search task](#) section earlier in this document.

The **Edit Task** pages are almost the same as the pages of the task creation wizard. The only difference is that the **Edit Task** pages display the current task settings, and then allows one to make and save changes to the selected task instead of creating a new one.

- **Create a new search task by copying an existing one** - Right-click the task to copy, click **Duplicate Task**, and then follow the steps to create a new task as listed in the [Creating and](#)

[configuring a new search task](#) section earlier in this document.

The **Duplicate Task** pages are almost the same as the pages of the task creation wizard. The only difference is that the **Duplicate Task** pages are pre-populated with the settings copied from the selected task.

- **Delete a given task** - First ensure that the task does not have any reports. Double-click the task to view a list of the task's reports, and then delete all reports from that list: Press Ctrl+A to select all reports, right-click the selection, and then click **Delete Reports** on the shortcut menu. Having deleted all reports, click **Tasks** in the console tree to return to the list of tasks, right-click the task, and then click **Delete**.

## Exporting and importing tasks

One can export search tasks to a file and then import them from the export file. This function may be useful, for example, when copying tasks to another server. It is possible to export a single task or all tasks.

### *To export a task*

1. In the console tree, select **DeviceLock Content Security Server > Search Server > Tasks**.
2. In the details pane, right-click the task to export, click **Export Task**, and specify the export file in the dialog box that appears.

### *To export all tasks*

1. In the console tree, select **DeviceLock Content Security Server > Search Server**.
2. In the details pane, right-click **Tasks**, click **Export All Tasks**, and specify the export file.

### *To import tasks from an export file*

1. In the console tree, select **DeviceLock Content Security Server > Search Server**.
2. In the details pane, right-click **Tasks**, click **Import Tasks**, and select the export file.

## Managing a task and its reports

The console displays search tasks in the console tree under **DeviceLock Content Security Server > Search Server > Tasks**. The shortcut menu on a search task in the console tree provides the same commands as the task's menu in the details pane (see [Managing existing tasks](#)).

When a search task is selected in the console tree, the details pane lists the reports produced by that task. The list in the details pane displays the following information on each report:

- **Name** - Report name includes the task name followed by the date and time of the task run.
- **Type** - Can be **Scheduled** or **Manual**, depending on whether the task was run by a schedule or by hand, respectively.
- **Status** - One of the following:
  - **Generating** - Report creation is in progress.
  - **Ready** - Report created successfully.
  - **Error** - Report encountered an error.

- **Results Found** - Number of items found by the search.
- **E-mailed** - One of the following:
  - **Yes** - Report successfully delivered to some or all of the intended e-mail recipients.
  - **No** - Report has no e-mail recipients or was not delivered to any of the intended e-mail recipients.
- **Started** - Date and time that the report creation started.
- **Finished** - Date and time that the report creation was completed.
- **Scheduled by** - Identifies the user account that started the task.
- **Scheduled from** - Identifies the computer from which the task was started.

To manage a report, right-click the report in the details pane and use the following commands from the shortcut menu that appears:

- **Open** - Displays the report in the details pane.  
Another way to open a task's report is by selecting the report under the node representing that task in the console tree.
- **Send via e-mail** - Sends the report to the e-mail recipients that were set in the dialog box displayed by this command.  
This command is available on the reports with the status of **Ready**, provided that the mail server is specified (see [Specifying mail server for Search Server reports](#)).
- **Rename** - Changes the name of the selected report.
- **Delete Report** - Deletes the selected report.  
One can delete multiple reports at a time: Click while holding down Shift or Ctrl to select reports, right-click the selection, and then click **Delete Reports**.
- **Refresh** - Updates the list of reports with the latest information.

The reports produced by a given search task are also listed under the node representing that task in the console tree. For example, if the name of the task is **Office Search**, the console tree lists the reports of that task under **DeviceLock Content Security Server > Search Server > Tasks > Office Search**. The details pane lists those reports when **Office Search** is selected in the console tree.

To open a report, do either of the following:

- Click the report in the console tree.
- Double-click the report in the details pane.

## Viewing a task's report

When one expands the node representing a search task in the console tree, and selects a report under that node, the details pane displays report pages that are very similar to the search result pages of the **Search Page** node. Another way to view a report is by using the **Open** command on the shortcut menu or by double-clicking the report list item in the details pane. The shortcut menu on a report in the console tree provides the same commands as the report's menu in the details pane (see [Managing a task and its reports](#)).

Each report page includes a heading and a list of search results.



The report heading displays the report name and ID number along with the following information:

- **Started** - Date and time that the report creation started.
- **Finished** - Date and time that the report creation was completed.
- **User** - Identifies the account that started the search task.
- **Computer** - Identifies the computer from which the search task was started.
- **Results found** - Number of items found by the search.
- **Results reported** - Number of items included in the report.  
**Results reported** may differ from **Results found** if the task is configured to limit the number of items in the report or the search found more than 100,000 items.
- **Search Options** - Click the **Search Options** button to view the settings of the search query performed by the task.  
The **Search Options** area lists only the configured settings, with the same setting names as in the task creation wizard. The empty settings are not displayed to prevent them from cluttering up the report heading.

List of search results includes the same areas as the list on the search result pages of the **Search Page** node:

- Statistics bar - Shows the number of results displayed on the current report page.
- Search results - Displays a numbered list of items containing information that matched the search criteria. See [Search results](#) for details on the list of search results.
- Results navigator - Shows how many report pages are returned and allows one to navigate from page to page.

Reports delivered via e-mail are the same as reports in the console with the only differences as follows: e-mailed reports are not divided into pages and they do not provide the ability to access shadow data from the list of search results.

The console redacts the Shadow Log related search results unless the console user is a DeviceLock Content Security Server administrator with the right to access shadow data. If the user does not have that right, the console replaces the shadow search results with asterisks. In e-mailed reports, the shadow search results are redacted if the user who initiates sending the report does not have the right to access shadow data. For an e-mailed report to disclose shadow search results, the following conditions are required:

- If the task e-mails the report, the user who runs that task by using the **Run Task** command in the console must have the right to access shadow data.
- The user who e-mails the report by using the **Send via e-mail** command in the console must have the right to access shadow data.

## Viewing and managing the tasks log

The tasks log provides information about events such as task creation, modification, and deletion; search start and finish (including the number of items found); and any errors that occur during task management or execution.

When **DeviceLock Content Security Server > Search Server > Tasks > Log Viewer** is selected in the console tree, the console lists events with the following information on each one:

- **Type** - Event type indicates one of the following:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Date/Time** - Date and time that the event occurred.
- **Event** - Identifies the event ID number.
- **Task Name** - Identifies the search task that caused the event.
- **Information** - A description of the event that includes details of the actions performed and errors encountered.
- **Server** - Identifies the computer on which the event has occurred.
- **Record N** - Sequence number of the event record in the list.

To manage the log, right-click in the list of events, and then use the following commands from the shortcut menu that appears:

- **Settings** - View or change the settings that limit the maximum number of event records the log may contain. See also [Managing log settings](#).
- **Save** - Saves the log to a file. The console prompts for the file name and location.
- **Refresh** - Updates the list of events with the latest information.
- **Filter** - Display only the events that match the conditions set. See also [Filtering the log](#).
- **Quick filters** - Point to this command and then click one of the following to limit the list to the events that occurred during:
  - **Current day** - Shows the events logged during the current calendar day.
  - **Current week** - Shows the events logged during the current calendar week.
  - **Current month** - Shows the events logged during the current calendar month.
  - **Current year** - Shows the events logged during the current calendar year.

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter** - Show all records by disabling the currently applied filter.
- **Clear** - Deletes all events in the tasks log. Also adds a deletion event to the tasks log, indicating the number of events that were deleted.

## Managing log settings

Use the following steps to view or change search the tasks log settings:

1. Select **DeviceLock Content Security Server > Search Server > Tasks > Log Viewer** in the console tree, right-click in the details pane, and then click **Settings**.
2. In the dialog box that appears, view, or change the following settings:
  - **Control log size** - Select this check box to allow the server to control the number of records in the log and delete outdated records. If this check box is cleared, the server uses all available database space to store the log.
  - **Keep events for last <number> days** - Select this option to store records no older than a certain number of days. Then, specify the desired number of days. The default setting is 365 days.
  - **Maximum log size: <number> records** - Select this option to store no more than a certain number of records. Then, specify the desired number of records, and select the server action to be performed when the log reaches the maximum size:
    - **Overwrite events as needed** - New event records continue to be stored when the maximum log size is reached. Each record of a new event replaces the oldest record in the log.
    - **Overwrite events older than <number> days** - New event records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.
    - **Do not overwrite events (clear log manually)** - New event records are not added when the maximum log size is reached. To enable the server to add new records, the log must be cleared by hand.

---

### Important

If the log has no space for new records and log settings do not allow the deletion of old records, then the server does not add any new records to the log.

---

To use the default log size, select the option **Maximum log size** and click **Restore Defaults**. The default log size settings are as follows:

- Maximum log size: 10,000 records
  - Overwrite events older than 7 days
3. When finished, click to **OK**.

## Filtering the log

Use the following steps to configure a filter for the search tasks log viewer:

1. Select **DeviceLock Content Security Server > Search Server > Tasks > Log Viewer** in the console tree, right-click in the details pane, and then click **Filter**.
2. In the dialog box that appears, use the following settings to configure a filter:
  - **Include** - The console lists only the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab.
  - **Exclude** - The console does not list the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab.

---

**Note**

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

- **Event types** - Select check boxes to filter events by type:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Task name, Information, Server, Event ID** - Include or exclude events depending upon whether event data matches the filter string specified.  
For example, to filter events by task name, specify a filter string in the **Task name** field. To filter events with certain IDs, enter ID numbers separated by a semicolon in the **Event ID** field.

---

**Note**

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

- **From** - Specify the beginning of the range of events to filter. Select **First Record** to filter events starting from the earliest one recorded in the log. Select **Records On** to filter events that occurred no earlier than a specific date and time.
- **To** - Specify the beginning of the range of events to filter. Select **Last Record** to filter events up to the latest one recorded in the log. Select **Records On** to filter events that occurred no later than a specific date and time.

3. When finished, click to **OK**.

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

Another option to narrow down the list of events is by using a quick filter:

- Select **DeviceLock Content Security Server > Search Server > Tasks > Log Viewer** in the console tree, right-click in the details pane, point to **Quick filters**, and then select one of the following options:
  - **Current day** - Shows the events logged during the current calendar day.
  - **Current week** - Shows the events logged during the current calendar week.
  - **Current month** - Shows the events logged during the current calendar month.
  - **Current year** - Shows the events logged during the current calendar year.

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

## Refreshing the list of events, saving and clearing the log

When viewing the log, one can also:

- Update the list of events with the most recent information - Select **DeviceLock Content Security Server > Search Server > Tasks > Log Viewer** in the console tree, right-click in the details pane, and then click **Refresh**.
- Save the log to a text file - Select **DeviceLock Content Security Server > Search Server > Tasks > Log Viewer** in the console tree, right-click in the details pane, click **Save**, and then use the dialog box that appears to specify the file.
- Delete all records from the log - Select **DeviceLock Content Security Server > Search Server > Tasks > Log Viewer** in the console tree, right-click in the details pane, and then click **Clear**. The **Clear** command records an event to the tasks log informing about the deletion and indicating the number of records that were deleted.

## File Formats Indexed for Search

Search Server can recognize, index, and search documents in the following file formats:

- Adobe Framemaker MIF (\*.mif)
- Adobe Photoshop images (metadata only) (\*.psd)
- Ami Pro (\*.sam)
- Ansi Text (\*.txt)
- Apple iWork KeyNote 2009 (\*.key)
- Apple iWork Numbers 2009 (\*.numbers)
- Apple iWork Pages 2009 (\*.pages)
- ASCII Text
- ASF media files (metadata only) (\*.asf)
- CSV (Comma-separated values) (\*.csv)
- DBF (\*.dbf)

- EBCDIC
- EML (emails saved by Outlook Express) (\*.eml)
- Enhanced Metafile Format (\*.emf)
- EMF Spool (\*.spl)
- Eudora MBX message files (\*.mbx)
- Flash (\*.swf)
- GZIP (\*.gz)
- Hancom Hanword (\*.hwp)
- Hancom Hanword 97 (\*.hwp)
- HTML (\*.htm, \*.html)
- iCalendar (\*.ics)
- Ichitaro (versions 5 and later) (\*.jtd, \*.jbw)
- JPEG (\*.jpg)
- Lotus 1-2-3 (\*.123, \*.wk?)
- MBOX email archives, including attachments (\*.mbx)
- MHT web page archives (\*.mht)
- MIME messages, including attachments
- MSG (emails saved by Outlook), including attachments (\*.msg)
- Microsoft Access 95, 97, 2000, 2003, 2007, 2010, 2013, 2016 MDB (\*.mdb, \*.accdb)
- Microsoft Document Imaging (\*.mdi)
- Microsoft Excel for Mac 2.2, 3, 4, 5, 98, 2001, X, 2004, 2008, 2011
- Microsoft Excel for Windows 2, 3, 4, 5
- Microsoft Excel 95, 97, 2000, XP, 2003, 2007, 2010, 2013, 2016 (\*.xls)
- Microsoft Excel 2003 XML (\*.xml)
- Microsoft Excel Office Open XML 2007, 2010, 2013, 2016 (\*.xlsx)
- Microsoft OneNote 2007, 2010, 2013, 2016 (\*.one)
- Microsoft Outlook 97, 2000, 2003, 2007, 2010, 2013, 2016 data files, including attachments (\*.PST, \*.OST)
- Microsoft Outlook/Exchange Messages, Notes, Contacts, Appointments, and Tasks
- Microsoft Outlook Express 5 and 6 message stores (\*.dbx)
- Microsoft PowerPoint 3, 4, 95, 97, 98, 2000, 2001, 2002, 2003, 2004, 2007, 2008, 2010, 2011, 2013, 2016 (\*.ppt)
- Microsoft PowerPoint Office Open XML 2007, 2010, 2013, 2016 (\*.pptx)
- Microsoft Rich Text Format (\*.rtf)
- Microsoft Searchable Tiff (\*.tiff)
- Microsoft Word for DOS 1, 2, 3, 4, 5, 6 (\*.doc)
- Microsoft Word for Mac 1, 3, 4, 5, 6, 98, 2001, X, 2004, 2008, 2011
- Microsoft Word for Windows 1, 2, 6 (\*.doc)
- Microsoft Word 95, 97, 98, 2000, 2002, 2003, 2007, 2010, 2013, 2016 (\*.doc)
- Microsoft Word 2003 XML (\*.xml)

- Microsoft Word Office Open XML 2007, 2010, 2013, 2016 (\*.docx)
- Microsoft Works WP (\*.wks)
- MP3 (metadata only) (\*.mp3)
- Multimate Advantage II (\*.dox)
- Multimate version 4 (\*.doc)
- OpenOffice/LibreOffice versions 1, 2, 3, 4, and 5 documents, spreadsheets, and presentations (\*.sxc, \*.sxd, \*.sxi, \*.sxw, \*.sxc, \*.stc, \*.sti, \*.stw, \*.stm, \*.odt, \*.ott, \*.odg, \*.otg, \*.odp, \*.otp, \*.ods, \*.ots, \*.odf)
- PDF files (\*.pdf)

---

#### **Note**

Encrypted PDF files can be indexed if the PDF file can be opened without a password and the PDF file permissions allow text extraction.

---

- PDF Portfolio files (\*.pdf), including embedded non-PDF documents
- Quattro Pro (\*.wb1, \*.wb2, \*.wb3, \*.qpw)
- QuickTime (\*.mov, \*.m4a, \*.m4v)
- RAR (\*.rar)
- TAR (\*.tar)
- TIFF (metadata only) (\*.tif)
- TNEF (winmail.dat)
- Treepad HJT files (\*.hjt)
- Unicode (UCS 16, Mac or Windows byte order, or UTF-8)
- Visio XML files (\*.vdx)
- Windows Metafile Format (\*.wmf)
- WMA media files (metadata only) (\*.wma)
- WMV video files (metadata only) (\*.wmv)
- WordPerfect 4.2 (\*.wpd, \*.wpf)
- WordPerfect (5.0 and later) (\*.wpd, \*.wpf)
- WordStar version 1, 2, 3, 4, 5, 6 (\*.ws)
- WordStar 2000
- Write (\*.wri)
- XBase, including FoxPro, dBase, and other XBase-compatible formats (\*.dbf)
- XML (\*.xml)
- XML Paper Specification (\*.xps)
- XSL
- XyWrite
- ZIP (\*.zip) (PKZIP 2.0-compatible)

# Appendix: Activating DeviceLock Licenses

This appendix provides information on how to license your copy of DeviceLock and its additional components with DeviceLock license files.

In this appendix:

[About DeviceLock License Types](#)

[Activating Client Licenses](#)

[Activating Server Licenses](#)

## About DeviceLock License Types

DeviceLock is licensed on a per-endpoint basis. The license specifies the number of endpoints on which it entitles you to set and enforce DeviceLock policies. From a license perspective, “endpoint” refers to any of the following:

- A laptop, desktop, or server
- A virtual machine
- A virtual desktop or application session

In the latter case, each session is considered a separate endpoint. The number of endpoints in your DeviceLock license should match the number of sessions hosted on your virtualization server. For example, when deploying DeviceLock on Remote Desktop Server, ensure that the number of endpoints in your DeviceLock license matches the number of remote desktop sessions hosted on the server.

As DeviceLock has a number of optional components, there are several license types:

License Type	License File Name
Core	devicelock.lic
ContentLock	dlcl.lic
NetworkLock	dlnl.lic
UAM (User Activity Monitor)	dluam.lic
Search Server	dlss.lic
Discovery Server	dl ds.lic
DeviceLock for Mac	dlmac.lic

The Core license is mandatory, the others relate to optional components. To use an optional component, its license must be activated in addition to the Core license. Without the Core license, the other licenses have no effect (except for the Discovery Server license).



If the Core license is missing, corrupt or has expired, then all DeviceLock components (except Discovery Server) operate in trial mode. Discovery Server does not require the Core license.

The number of ContentLock, NetworkLock and/or UAM licenses must match the number of Core licenses; otherwise, the respective components are deemed not licensed.

### **Example**

Suppose you have the following number of licenses activated on a computer running DeviceLock Management Console:

Core - 1,000; ContentLock - 1,000; NetworkLock - 1,000; UAM - 1,000.

Then, you activate 100 additional Core licenses on that computer, so the total number of Core licenses exceeds the number of ContentLock, NetworkLock, and UAM licenses:

Core - 1,100; ContentLock - 1,000; NetworkLock - 1,000; UAM - 1,000.

As a result, ContentLock, NetworkLock, and UAM switch into trial mode, so these components are no longer available for configuration and use.

The issue in this example can be resolved by activating 100 additional ContentLock, NetworkLock, and UAM licenses on the DeviceLock Management Console computer where 1,100 Core licenses are activated. Another option is to remove the 100 Core licenses from that computer and activate them on a different computer running the DeviceLock Management Console that has no ContentLock, NetworkLock, and UAM licenses. This DeviceLock Management Console will be able to control 100 computers, but without ContentLock, NetworkLock, and UAM features.

## Activating Client Licenses

To use DeviceLock, first activate the Core license. To use ContentLock, NetworkLock, and/or User Activity Monitor, activate the respective licenses in addition to the Core license.

The Core and DeviceLock for Mac licenses are activated on computers running DeviceLock Management Console or DeviceLock Enterprise Server, that is, on computers used to manage DeviceLock Service on other computers, or to collect data from computers controlled by DeviceLock Service.

To activate the Core or Device for Mac licenses, copy the file `devicelock.lic` or `dlmac.lic` (DeviceLock for Mac) to the DeviceLock installation folder, and then start DeviceLock Management Console to activate that file. By default, the DeviceLock installation folder is `%ProgramFiles%\DeviceLock` or `%ProgramFiles(x86)%\DeviceLock` on a 32-bit or 64-bit system, respectively.

The ContentLock, NetworkLock, and UAM licenses are activated on the same computers as the Core license. Copy the license files (such as `dlcl.lic`, `dlnl.lic`, and `dluam.lic`) to the DeviceLock installation folder, and then start DeviceLock Management Console to activate them.

When started, DeviceLock Management Console automatically recognizes the license files found in the DeviceLock installation folder, and activates the licenses accordingly. No additional actions are required.

---

**Note**

- The name of DeviceLock license files originally has the .lic extension. When a client license is activated, the extension changes to .li\_.
  - Multiple license files can be copied to the installation folder by assigning each of them a unique name. For example, device.lock.lic, device.lock1.lic, dlc1.lic, dlc12.lic, etc.
- 

**Recommendations**

After replacing an expired DeviceLock license file with a valid one, the About DeviceLock page in the management console may still display outdated license information. This problem is usually because the expired license file has been replaced by a valid one with the same name.

To resolve the issue, follow these steps:

1. Delete the license file from the DeviceLock installation folder. By default, the installation folder is %ProgramFiles%\DeviceLock Or %ProgramFiles(x86)%\DeviceLock on a 32-bit or 64-bit system, respectively.
2. Start the registry editor (regedit.exe). In the case of a 32-bit system, delete the registry value HKLM\SOFTWARE\SmartLine Vision\LIC. In the case of a 64-bit system, delete the registry value HKLM\SOFTWARE\Wow6432Node\SmartLine Vision\LIC.
3. Copy the new license file to the DeviceLock installation folder, and then start the DeviceLock Management Console to activate that file.

## Activating Server Licenses

DeviceLock Search Server and Discovery Server require additional licenses. DeviceLock Enterprise Server requires the DeviceLock Core license. The UAM license is required to collect user activity monitor data on DeviceLock Enterprise Server (see [Viewing User Activity](#)).

## Enterprise Server

DeviceLock Enterprise Server is an optional component that does not require an additional license. The existing Core license will suffice to install as many instances of this server as needed to distribute data load between them.

To collect DeviceLock Service logs, the Core license must be activated on DeviceLock Enterprise Server.

To apply ContentLock and/or NetworkLock settings through server policies and computer monitoring tasks, the ContentLock and/or NetworkLock licenses must be activated on DeviceLock Enterprise Server.

To apply user activity monitor settings through server policies and computer monitoring tasks, the UAM license must be activated on DeviceLock Enterprise Server.

To activate a license, install the license file (such as device.lock.lic or dluam.lic) by using the DeviceLock Management Console as follows:

1. Connect the console to the DeviceLock Enterprise Server.
2. In the console tree, select **DeviceLock Enterprise Server** > [Server Options](#).
3. Double-click **DeviceLock license(s)** in the details pane and load the license file in the dialog box that appears.

## Search Server

Search Server (which is a part of DeviceLock Content Security Server) is used to index and search documents collected in DeviceLock Enterprise Server logs. To use Search Server, the license for that server must be activated in addition to activating the Core license on DeviceLock Enterprise Server.

To activate a Search Server license, install the license file (such as d1ss.lic) by using the DeviceLock Management Console as follows:

1. Connect the console to the DeviceLock Content Security Server.
2. In the console tree, select **DeviceLock Content Security Server** > [Server Options](#) > [Search Server Options](#).
3. Double-click **Search Server License(s)** in the details pane and load the license file in the dialog box that appears.

## Discovery Server

Discovery Server (which is a part of DeviceLock Content Security Server) is used to scan users' workstations and storage systems for certain types of content and data according to configurable rules. To use Discovery Server, the license for that server must be activated. The DeviceLock Core license is not required.

To activate a Discovery Server license, install the Discovery Server license file (such as d1ds.lic) by using the DeviceLock Management Console as follows:

1. Connect the console to the DeviceLock Content Security Server.
2. In the console tree, select **DeviceLock Content Security Server** > **Server Options** > **Discovery Server Options**.
3. Double-click **Discovery Server License(s)** in the details pane and load the license file in the dialog box that appears.

# Appendix: Consolidating the Logs in the Cloud Using OpenVPN

In this appendix:

- [Requirements Overview](#)
- [Configuring the Cloud Server](#)
- [Configuring On-premises Servers](#)

## Requirements Overview

When consolidating DeviceLock logs (see [Consolidating Logs](#)) in a local area network environment, servers exchange data by using remote procedure call (RPC) over Transmission Control Protocol/Internet Protocol (TCP/IP). This method provides quick and efficient communication in a corporate network.

Communication with a cloud server via RPC can be provided through a secure virtual private network (VPN) connection using OpenVPN software. In this appendix, you can find instructions on how to configure the OpenVPN server and client as well as the DeviceLock Enterprise Server to consolidate DeviceLock logs on a cloud server.

The following conditions are required to consolidate DeviceLock logs from designated on-premises servers to a cloud server through a VPN connection using OpenVPN:

- The on-premises servers can gain access to the cloud computer by its IP address.  
This requirement is met, for example, when the on-premises computer has Internet access, and the cloud computer has a static public IP address and thus is directly accessible over the Internet.
- On both the on-premises and cloud computers, Windows Firewall is configured so that:
  - Port 80 is open for inbound public TCP traffic.
  - The DeviceLock Enterprise Server is allowed inbound public TCP traffic.

To meet these requirements, use the “Windows Defender Firewall with Advanced Security” console (wf.msc) to create the inbound rules with the following settings:

- Rule type - Port; Protocol - TCP; Local port - 80; Action - Allow the connection; Profile - Public.
- Rule type - Program; Protocol - TCP; This program path - %ProgramFiles%(x86)\DeviceLock\DLServer.exe; Action - Allow the connection; Profile - Public.
- The OpenVPN server is installed and configured on the cloud computer.
- The OpenVPN client is installed and configured on the on-premises computer.
- DeviceLock Enterprise Server on both the cloud and on-premises computers is assigned a fixed network port. Normally, this is port 9133.
- The on-premises DeviceLock Enterprise Server uses a DeviceLock certificate to authenticate with the cloud-based DeviceLock Enterprise Server.

In this appendix, we assume that DeviceLock Enterprise Server is already installed, up and running on both the on-premise and cloud computers. Our object is to make the on-premises DeviceLock Enterprise Server a remote consolidation server for the DeviceLock Enterprise Server running in the cloud. As a result, the cloud server will consolidate logs from the on-premises one. In the same way, you can configure log consolidation from multiple on-premises servers.

In addition, the configuration described here will enable the DeviceLock Management Console from the on-premises computer to connect and manage the cloud-based DeviceLock Enterprise Server.

## Configuring the Cloud Server

On the cloud computer, the OpenVPN server must be installed and configured, and the DeviceLock Enterprise Server must be prepared to handle consolidation requests from on-premises servers.

This section covers the following tasks to configure the cloud server:

- [Install OpenVPN](#)
- [Prepare the Server Certificates](#)
- [Configure the OpenVPN Server](#)
- [Configure the DeviceLock Enterprise Server](#)

### Install OpenVPN

Download the OpenVPN installer .exe file for Windows from the site at [openvpn.net/community-downloads](https://openvpn.net/community-downloads). Run the installer .exe file and follow the steps in the Setup wizard that appears:

- Select all components to install, including **EasyRSA 2 Certificate Management Scripts**. You will need this component to build the certificates.
- Accept the default installation folder, %ProgramFiles%\OpenVPN. This folder will also store the configuration of the OpenVPN server.
- When prompted, agree to install the TAP device software. This virtual network device provides connection and data exchange between the OpenVPN server and its clients.
- OpenVPN requires Microsoft .NET Framework 4.0 or later. If prompted by the Setup wizard, install the latest version of the .NET Framework. For installation instructions, see Microsoft's article at [docs.microsoft.com/dotnet/framework/install](https://docs.microsoft.com/dotnet/framework/install).

Once you have completed the Setup wizard, you can move on to configure the server.

### Prepare the Server Certificates

OpenVPN provides tools to prepare certificates and other items for authentication and encryption purposes. Certificates are required, in particular, to ensure the security of the communication channel between the on-premises server and the cloud server. The certificate management tools are in the folder %ProgramFiles%\OpenVPN\easy-rsa.

On the cloud computer, open a command prompt as an administrator, and enter the following commands to configure the initial values for the certificate management tools:

```
cd "%ProgramFiles%\OpenVPN\easy-rsa"
```

```
init-config.bat
```

These commands create the `vars.bat` file in the `easy-rsa` folder with the initial values for building certificates. Open the `vars.bat` file in Notepad to view or change those values. In this file, you could set the values for the certificate fields, such as `KEY_COUNTRY`, `KEY_PROVINCE`, `KEY_CITY`, etc. These values are used by default, and can be changed when building a certificate.

Enter the following commands to create the Certification Authority (CA) certificate:

```
vars.bat
```

```
clean-all.bat
```

```
build-ca.bat
```

When asked for input, accept or change the default values apart from the `Name` and `Common name` fields. In these fields, enter the `ca` value:

```
Common name: ca
```

```
Name: ca
```

Next, build a certificate and a private key for the OpenVPN server. Enter the following command at the command prompt:

```
build-key-server.bat server
```

When asked for input, accept or change the default values apart from the `Name` and `Common name` fields. In these fields, enter the `server` value:

```
Common name: server
```

```
Name: server
```

To complete the setup of encryption, prepare the Diffie Hellman parameters. Enter the following command at the command prompt:

```
build-dh.bat
```

As a result of these commands, the following files will appear in the `easy-rsa\keys` folder: `ca.crt`, `server.crt`, `server.key`, `dh2048.pem`.

## Configure the OpenVPN Server

First, copy the certificates you have prepared (see [Prepare the Server Certificates](#)) to the OpenVPN server configuration folder. On the cloud computer, open a command prompt as an administrator, and enter the following commands:

```
cd "%ProgramFiles%\OpenVPN\easy-rsa\keys"
```

```
copy ca.crt "%ProgramFiles%\OpenVPN\config"
```

```
copy server.crt "%ProgramFiles%\OpenVPN\config"
```

```
copy server.key "%ProgramFiles%\OpenVPN\config"
```

```
copy dh2048.pem "%ProgramFiles%\OpenVPN\config"
```

Next, run the following commands to prepare the server configuration file:

```
cd "%ProgramFiles%\OpenVPN\sample-config"
```

```
copy server.ovpn "%ProgramFiles%\OpenVPN\config"
```

Now you need to edit the server configuration file, which is much easier to do with Notepad++. You could download and install Notepad++ from the site at [ninite.com/notepadplusplus](https://ninite.com/notepadplusplus). Then, open the configuration file to edit:

```
cd "%ProgramFiles%\OpenVPN\config"
```

```
"%ProgramFiles%\Notepad++\notepad++.exe" server.ovpn
```

- or -

```
"%ProgramFiles(x86)%\Notepad++\notepad++.exe" server.ovpn
```

Edit the configuration file by setting the following parameter values:

```
local 0.0.0.0
```

```
port 80
```

```
proto tcp
```

```
;proto udp
```

Put a semicolon at the beginning of the line to disable this parameter.

```
ifconfig-pool-persist ip.txt
```

```
;tls-auth ta.key 0
```

Put a semicolon at the beginning of the line to disable this parameter.

```
;explicit-exit-notify 1
```

Put a semicolon at the beginning of the line to disable this parameter.

Note that the subnet from which OpenVPN picks IP addresses is set by the server parameter:

```
server 10.8.0.0 255.255.255.0
```

With this parameter value, the OpenVPN server is assigned the IP address of 10.8.0.1, and the remaining IP addresses from this subnet can be assigned to the OpenVPN clients.

Finally, configure the OpenVPN server to start automatically when the system starts. Use the Services console (services.msc) to set the startup type of the service OpenVPNService to Automatic. Then, start that service.

## Configure the DeviceLock Enterprise Server

On the cloud computer, configure the DeviceLock Enterprise Server as follows:

- Install the private key of a DeviceLock certificate by using the **DeviceLock certificate** parameter in [Server Options](#).
- Assign a fixed port to the server, such as port 9133, by using the **TCP port** parameter in [Server Options](#).

## Configuring On-premises Servers

On the on-premises computer, the OpenVPN client must be installed and configured to connect to the OpenVPN server that runs on the cloud computer. When connecting, the OpenVPN server shall assign a certain fixed IP address to the client. The DeviceLock Enterprise Server on the on-premises computer must be configured to transfer DeviceLock logs to the cloud server.

This section covers the following tasks to configure an on-premises server:

- [Install OpenVPN](#)
- [Prepare the Client Certificate and IP Address](#)
- [Configure the OpenVPN Client](#)
- [Configure the DeviceLock Enterprise Server](#)
- [Test: Connect the Console to the Cloud Server](#)

## Install OpenVPN

Download the OpenVPN installer .exe file for Windows from the site at [openvpn.net/community-downloads](https://openvpn.net/community-downloads). Run the installer .exe file and follow the steps in the Setup wizard that appears:

- Keep the default selection of the components to install, which does not install **EasyRSA 2 Certificate Management Scripts**. This component is not used on the client computers.
- Accept the default installation folder, %ProgramFiles%\OpenVPN. This folder will also store the configuration of the OpenVPN client.
- When prompted, agree to install the TAP device software. This virtual network device provides connection and data exchange between the OpenVPN client and server.
- OpenVPN requires Microsoft .NET Framework 4.0 or later. If prompted by the Setup wizard, install the latest version of the .NET Framework. For installation instructions, see Microsoft's article at [docs.microsoft.com/dotnet/framework/install](https://docs.microsoft.com/dotnet/framework/install).

Once you have completed the Setup wizard, you can move on to configure the client.

## Prepare the Client Certificate and IP Address

Each OpenVPN client requires a certificate with a unique name. This could be, for example, the name of the on-premises computer.

Perform the following steps to create the certificate for the OpenVPN client:

1. On the cloud computer where the OpenVPN server is installed, open a command prompt as an administrator.



2. At the command prompt, enter the following commands:

```
cd "%ProgramFiles%\OpenVPN\easy-rsa"
```

```
vars.bat
```

```
build-key.bat <computer name>
```

In the last command, <computer name> stands for the name of the on-premises computer to run the OpenVPN client.

When asked for input, accept or change the default values apart from the Name and Common name fields. In these fields, enter the name of the on-premises computer:

```
Common name: <computer name>
```

```
Name: <computer name>
```

As a result of these commands, the files <computer name>.crt and <computer name>.key appear in the folder easy-rsa\keys. You should copy these two files along with the file ca.crt to the client's configuration folder on the on-premises computer (%ProgramFiles%\OpenVPN\config).

The OpenVPN server must be configured to assign a certain fixed IP address to the OpenVPN client. This IP address is associated with the name of the client's certificate, which in our case is the name of the on-premises computer.

Due to a known limitation of the TAP driver in the case of the routed IP tunnel, the host number in the client IP address must be such that the remainder of dividing it by 4 is 2. For example, if the subnet from which OpenVPN picks addresses has the start IP address of 10.8.0.0 with the network mask 255.255.255.0 (set by the server parameter in the OpenVPN server configuration file), then a valid client address could be 10.8.0.6, 10.8.0.10, 10.8.0.14, 10.8.0.18, and so on.

Perform the following steps to assign a fixed IP address to the on-premises computer running the OpenVPN client:

1. On the cloud computer where the OpenVPN server is installed, open a command prompt as an administrator.

2. At the command prompt, enter the following commands:

```
net stop OpenVPNService
```

```
cd "%ProgramFiles%\OpenVPN\config"
```

```
notepad ip.txt
```

3. In the file ip.txt, add a line composed of the client's certificate name followed by a comma and the desired IP address. For example:

```
mycomp,10.8.0.6
```

---

### Important

- To edit the file `ipp.txt`, the OpenVPN server must be stopped. This condition is ensured with the command `net stop OpenVPNService`. When finished editing, start that service (for example, by entering `net start OpenVPNService` at a command prompt).
  - Having started, the OpenVPN server updates the file `ipp.txt` to align the client IP address assignment with the TAP driver requirements, subtracting 2 from the actual host number. For example, for a client with the IP address of `10.8.0.6`, the IP address set in the file `ipp.txt` would be `10.8.0.4`.
- 

## Configure the OpenVPN Client

When preparing the client certificate (see [Prepare the Client Certificate and IP Address](#)), the files `<computer name>.crt` and `<computer name>.key` were created in the folder `easy-rsa\keys` on the cloud computer. Copy these two files along with the file `ca.crt` to the client's configuration folder `%ProgramFiles%\OpenVPN\config` on the on-premises computer.

Next, on the on-premises computer, open a command prompt as an administrator, and enter the following commands to prepare the client configuration file:

```
cd "%ProgramFiles%\OpenVPN\sample-config"

copy client.ovpn "%ProgramFiles%\OpenVPN\config"
```

Now you need to edit the client configuration file, which is much easier to do with Notepad++. You could download and install Notepad++ from the site at [ninite.com/notepadplusplus](https://ninite.com/notepadplusplus/). Then, open the configuration file to edit:

```
cd "%ProgramFiles%\OpenVPN\config"

"%ProgramFiles%\Notepad++\notepad++.exe" server.ovpn

- or -

"%ProgramFiles(x86)%\Notepad++\notepad++.exe" server.ovpn
```

Edit the configuration file by setting the following parameter values:

```
proto tcp
```

```
;proto udp
```

Put a semicolon at the beginning of the line to disable this parameter.

```
remote <cloud computer's public IP address> 80
```

Example: `remote 212.46.5.117 80`

```
cert <computer name>.crt
```

```
key <computer name>.key
```

```
;tls-auth ta.key 1
```

Put a semicolon at the beginning of the line to disable this parameter.

Finally, configure the OpenVPN client to start automatically when the system starts. Use the Services console (services.msc) to set the startup type of the service OpenVPNService to Automatic. Then, start that service.

## Configure the DeviceLock Enterprise Server

Configure the on-premises DeviceLock Enterprise Server as follows:

- Assign a fixed port to the server, such as port 9133, by using the **TCP port** parameter in [Server Options](#).
- Redirect the consolidation-related traffic of the on-premises DeviceLock Enterprise Server to the OpenVPN server on the cloud computer, and configure certificate-based authentication:
  1. Double-click the **Log consolidation** parameter in [Server Options](#).
  2. In the dialog box that appears, in the **Consolidation server** field, enter the IP address of the OpenVPN server.

This is the server address from the OpenVPN subnet defined by the server parameter in the server configuration file. Thus, with this parameter set to 10.8.0.0 255.255.255.0, the IP address of the OpenVPN server is 10.8.0.1.
  3. Click the button next to the **Consolidation server** field and supply the public key of the DeviceLock certificate in the dialog box that appears. This must be the certificate the private key of which is installed on the cloud server.
- Configure the sending of the client's IP address and port number to the cloud server:
  1. In the Windows Registry editor (regedit) on this on-premises computer, open the following registry key:  
HKLM\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer
  2. In this registry key, create a value with the following settings:
    - Name: SlaveRemoteAddress
    - Type: REG\_SZ
    - Data: The IP address of this OpenVPN client's IP address (such as 10.8.0.6) followed by a colon with the number of the port assigned to the DeviceLock Enterprise Server on this on-premises computer. Example: 10.8.0.6:9133

The on-premises server will have submitted this data to the cloud server when sending a consolidation request. In this way, the cloud server will become aware of the IP address and port for communicating with this on-premises server.

## Test: Connect the Console to the Cloud Server

Having configured OpenVPN, you can test it by connecting the on-premises console to the cloud server. Run the DeviceLock Management Console on the on-premises computer and connect to the DeviceLock Enterprise Server running in the cloud:

1. Start the DeviceLock Management Console on the on-premises computer.
2. In the console tree, right-click **DeviceLock Enterprise Server** and choose the **Connect** command.

3. In the dialog box that appears, click **Another computer**.
4. In the **Another computer** box, enter the IP address of the OpenVPN server on the cloud computer followed by the DeviceLock Enterprise Server's port number enclosed in brackets.  
Example: 10.8.0.1[9133]
5. Click **OK** and wait while the console establishes the connection.
6. Should the console prompt for a user name and password, enter the name and password of a user account with sufficient rights to access the DeviceLock Enterprise Server on the cloud computer.

With this VPN-connection, the console communicates with the cloud server by submitting RPC requests to the on-premises OpenVPN client. The client forwards requests to the cloud-based OpenVPN server that, in its turn, forwards them to the DeviceLock Enterprise Server.

# Appendix: Examples

In this appendix:

[Permission and Audit Examples for Devices](#)

[Permission Examples for Protocols](#)

[Content-Aware Rule Examples](#)

[Basic IP Firewall Rule Examples](#)

## Permission and Audit Examples for Devices

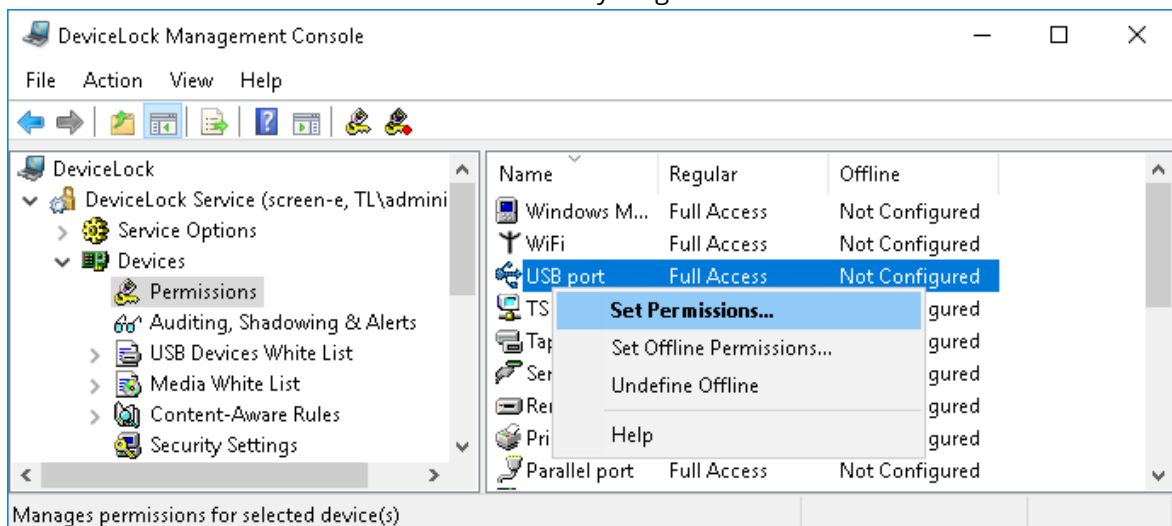
The following examples demonstrate how to properly define permissions, audit and shadowing rules in DeviceLock.

All examples assume you are using the DeviceLock Management Console connected to a computer running the DeviceLock Service. For more information on how to use the DeviceLock Management Console, see [DeviceLock Consoles and Tools](#).

### Permission Examples

***For all users all USB devices are denied except the mouse and keyboard:***

1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the shortcut menu available by a right mouse click.

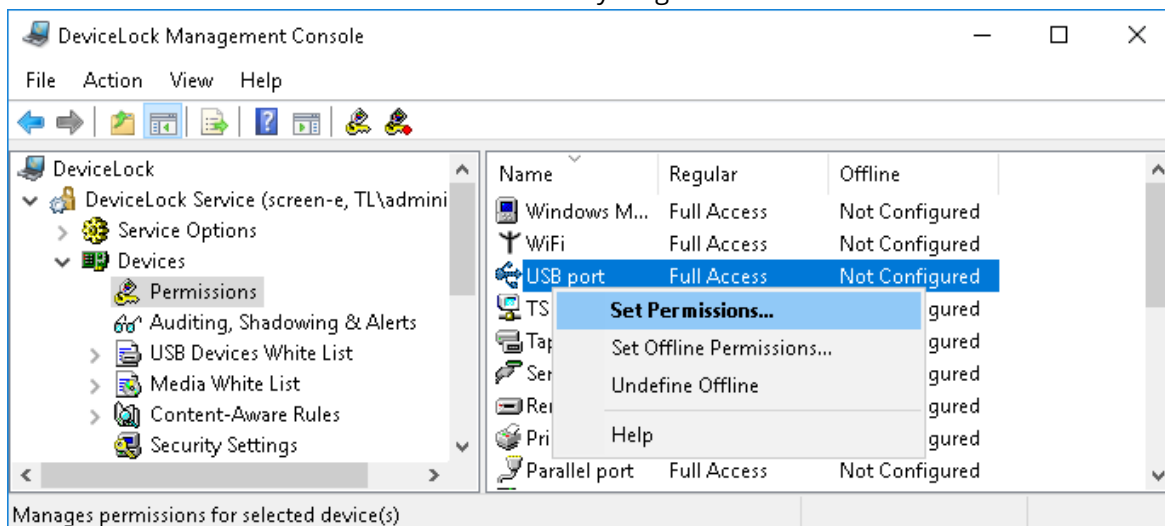


2. Click the **Add** button in the **Permissions** dialog box, add the **Everyone** user (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.

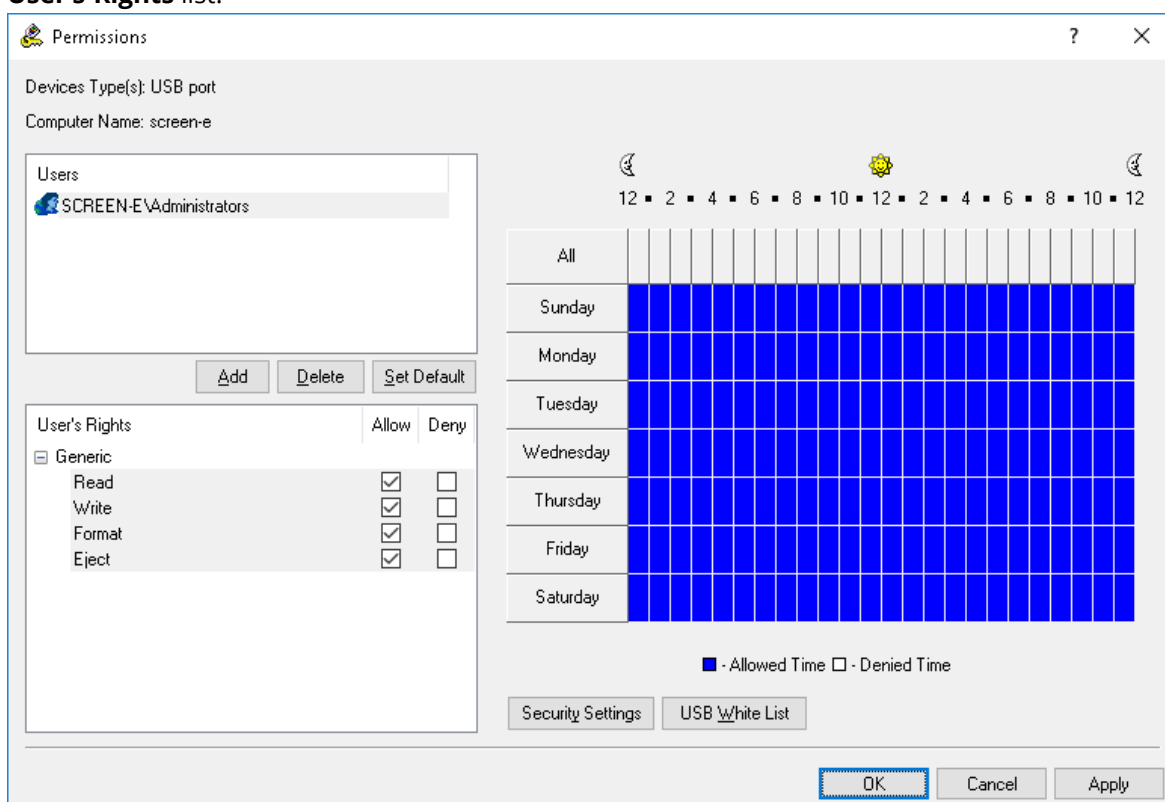


**For all users all USB devices are denied except the mouse and keyboard but the Administrators group can use any USB devices:**

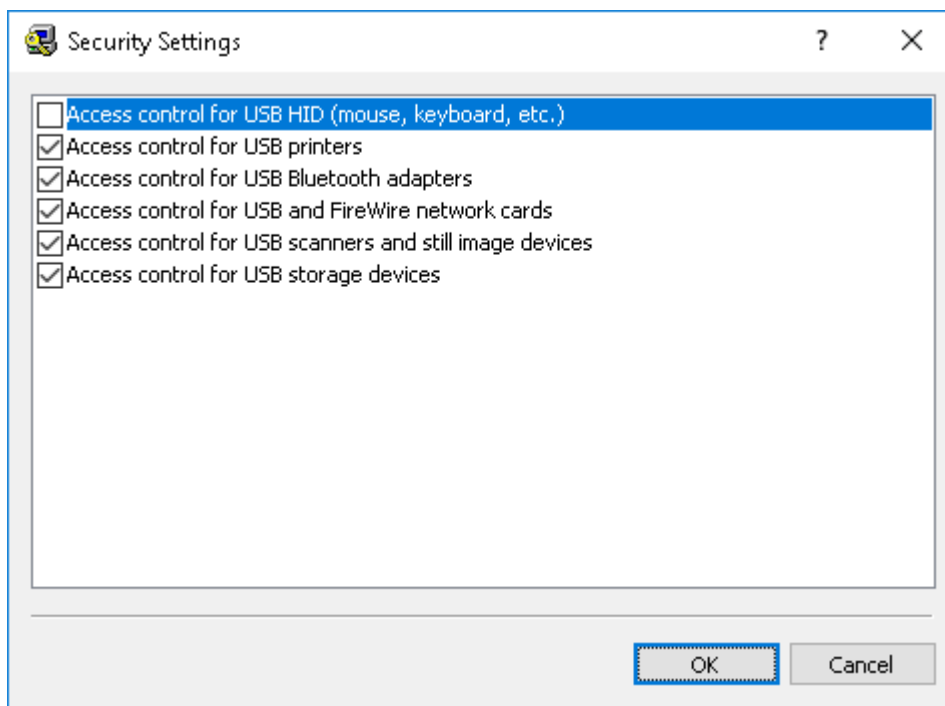
1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the shortcut menu available by a right mouse click.



2. Click the **Add** button in the **Permissions** dialog box, add the **Administrators** group (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, select the **Administrators** record and enable all rights in the **User's Rights** list.



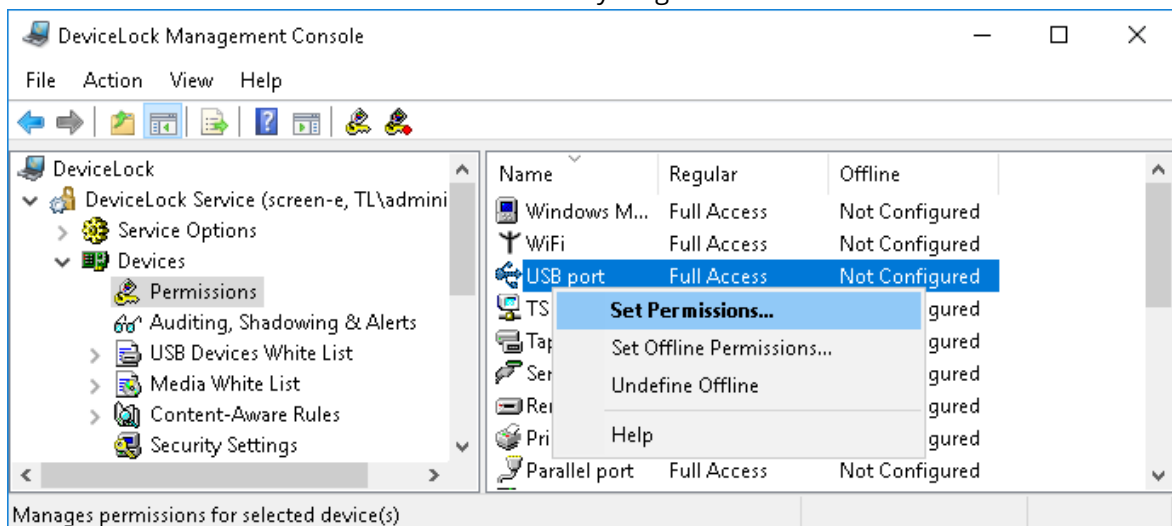
3. Click the **Security Settings** button in the **Permissions** dialog box, and then clear the **Access control for USB HID (mouse, keyboard, etc.)** check box.



4. Click **OK** to close the **Security Settings** dialog box, and then click **OK** to apply changes and close the **Permissions** dialog box.

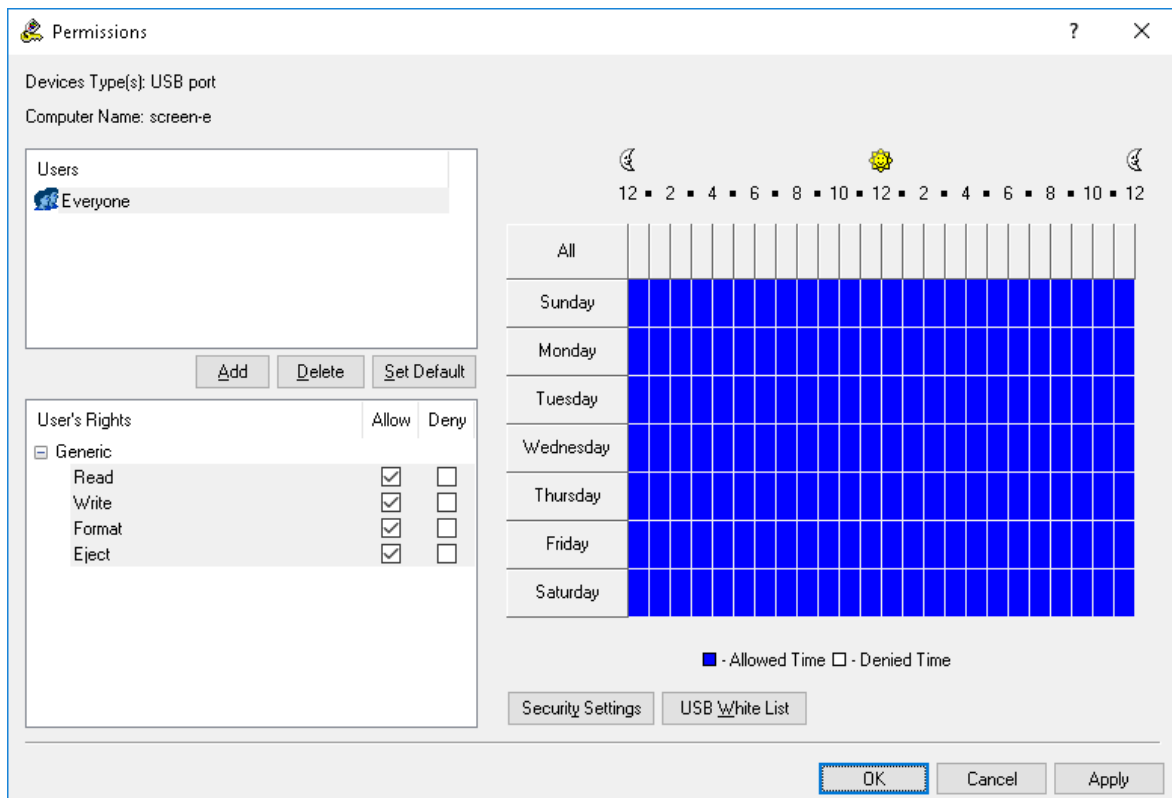
***For all users all storage devices except fixed hard disk drives are denied but all non-storage USB devices are allowed:***

1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the shortcut menu available by a right mouse click.

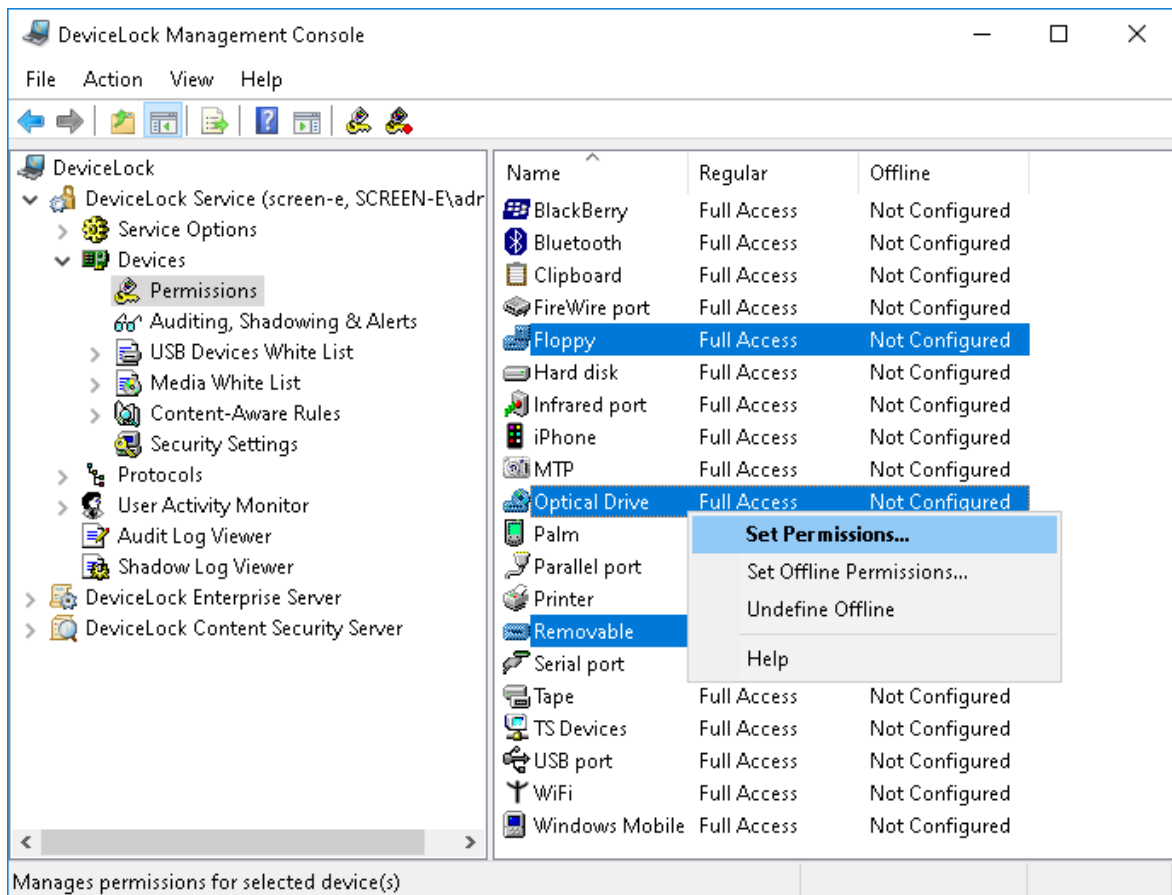


2. Click the **Add** button in the **Permissions** dialog box, add the **Everyone** user (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and enable all rights in the **User's Rights** list.

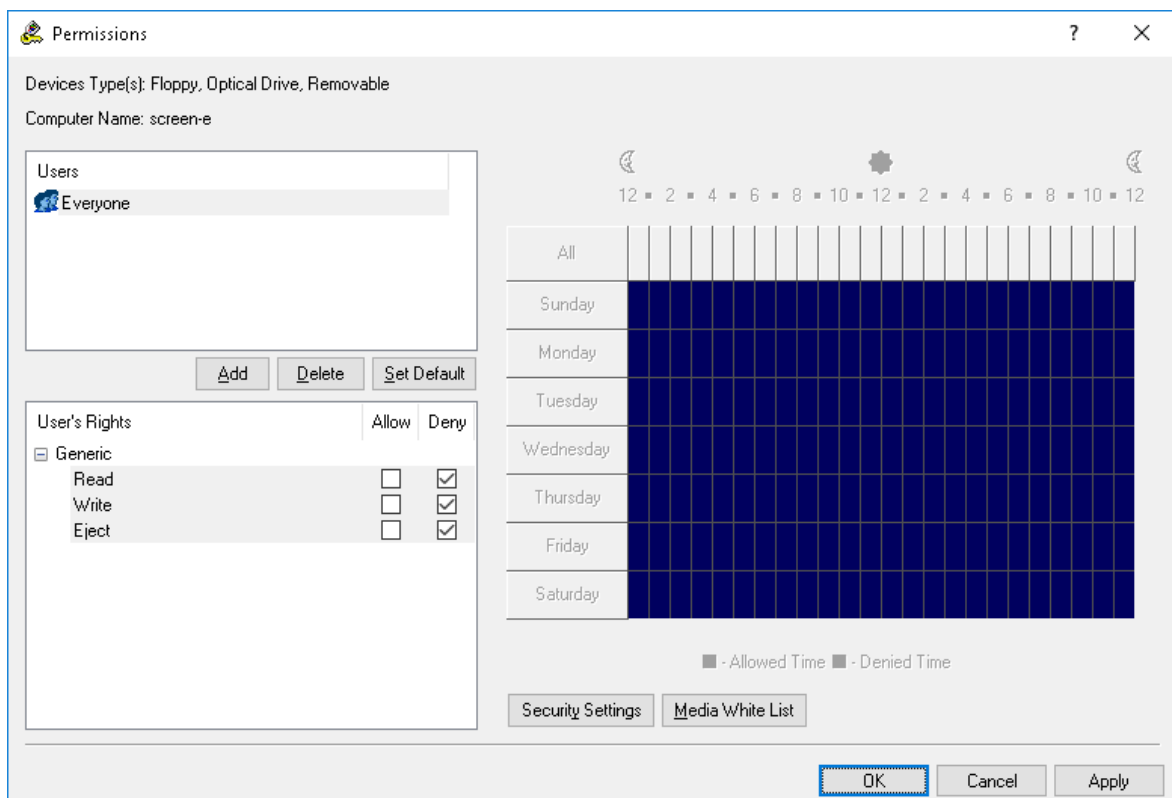




3. Click **OK** to apply changes and close the **Permissions** dialog box.
4. Select the **Floppy**, **Optical Drive**, and **Removable** device types in the **Permissions** node, and then select **Set Permissions** from the shortcut menu available by a right mouse click.



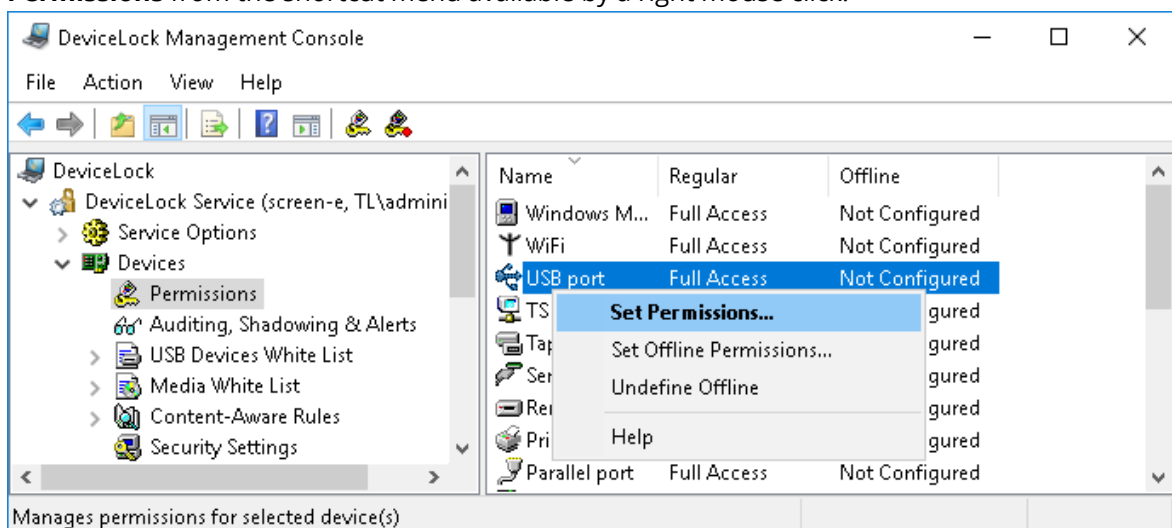
- Click the **Add** button in the **Permissions** dialog box, add the **Everyone** user (type the name or browse for all available names and select the needed one), click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.



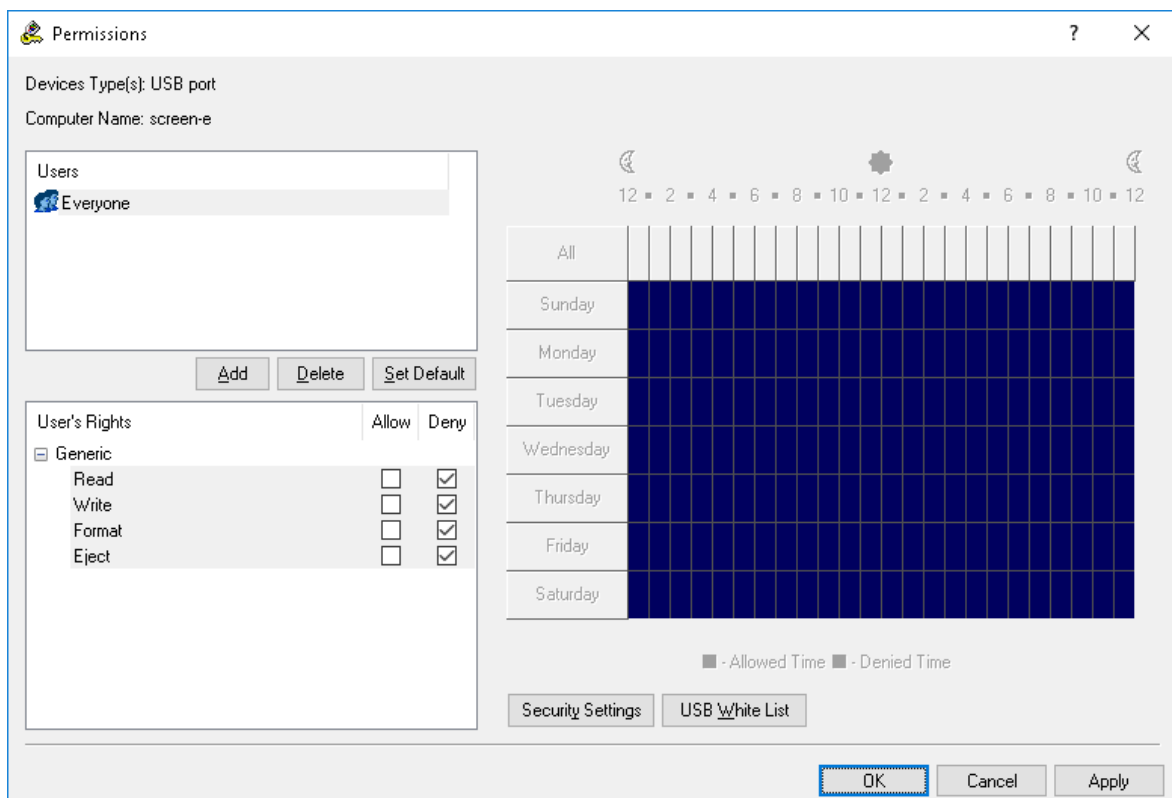
- Click **OK** to apply changes and close the **Permissions** dialog box, and then click **Yes** to confirm that you really want to deny access to these devices for all users.

***For all users all USB devices are denied except the mouse and keyboard but the Administrators group can use a certain model of USB storage devices:***

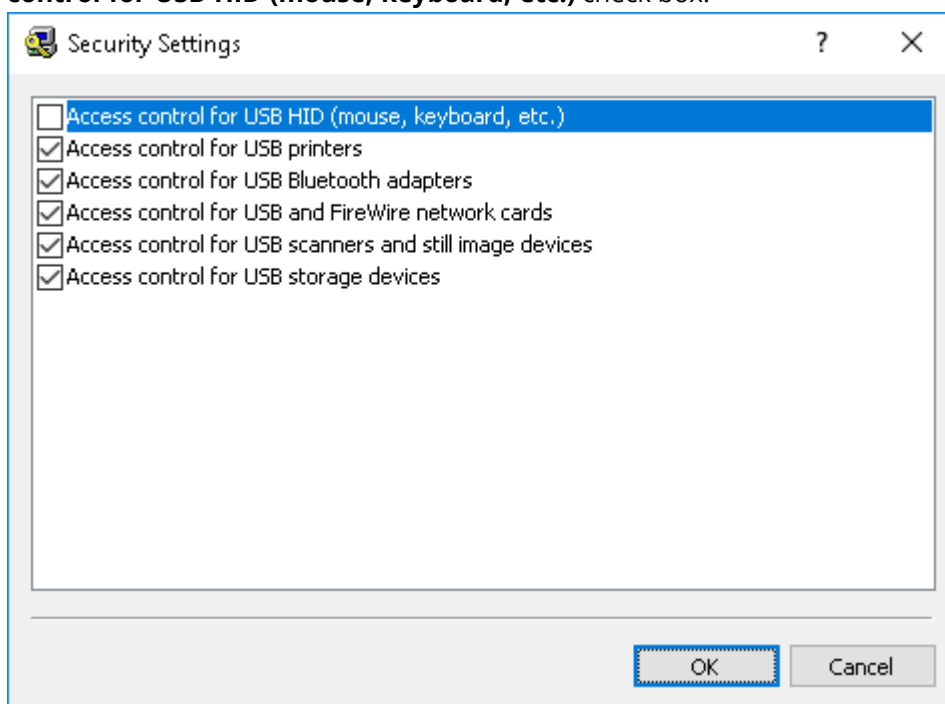
- Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the shortcut menu available by a right mouse click.



- Click the **Add** button in the **Permissions** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.

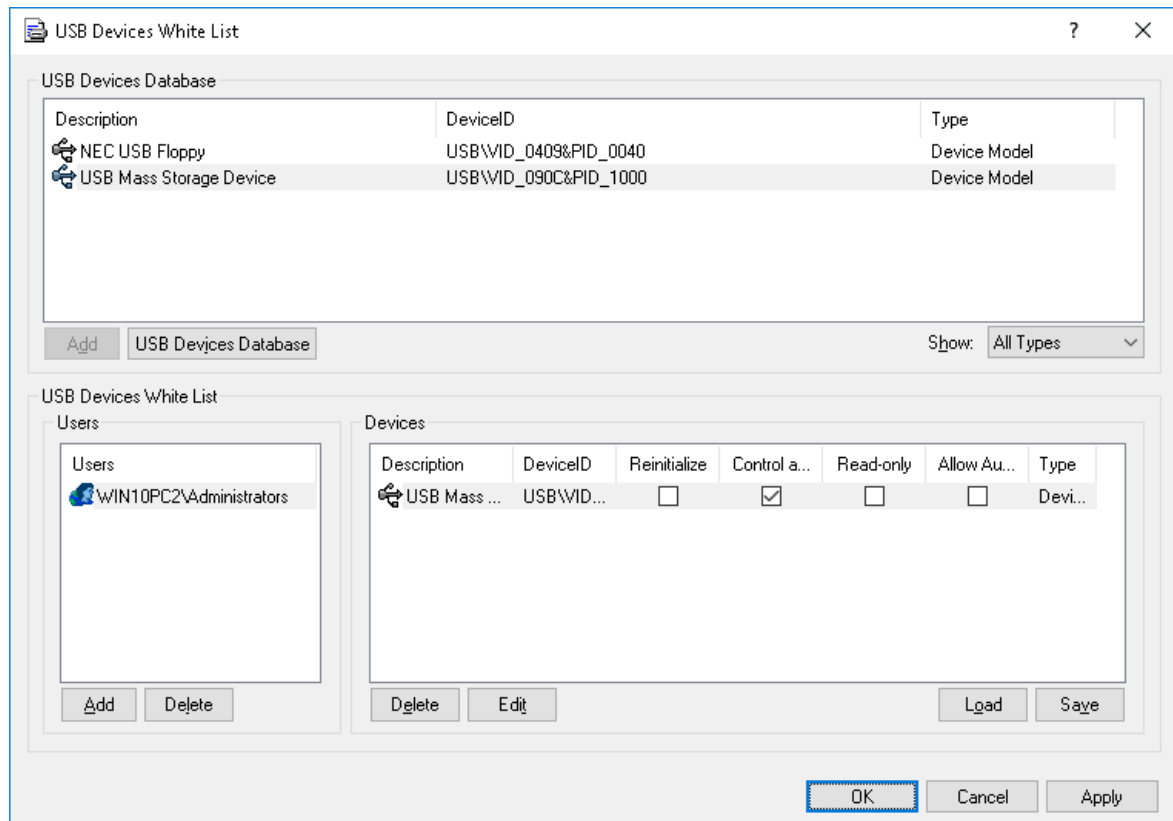


3. Click the **Security Settings** button in the **Permissions** dialog box, and then clear the **Access control for USB HID (mouse, keyboard, etc.)** check box.



4. Click **OK** to close the **Security Settings** dialog box
5. Click the **USB White List** button in the **Permissions** dialog box.
6. In the **USB Devices White List** dialog box that appears, click the **Add** button below the **Users** list and add the **Administrators** group (type the name or browse for all available names and select

the needed one). Click **OK** to close the **Select Users or Groups** dialog box, and then select the **Administrators** record.



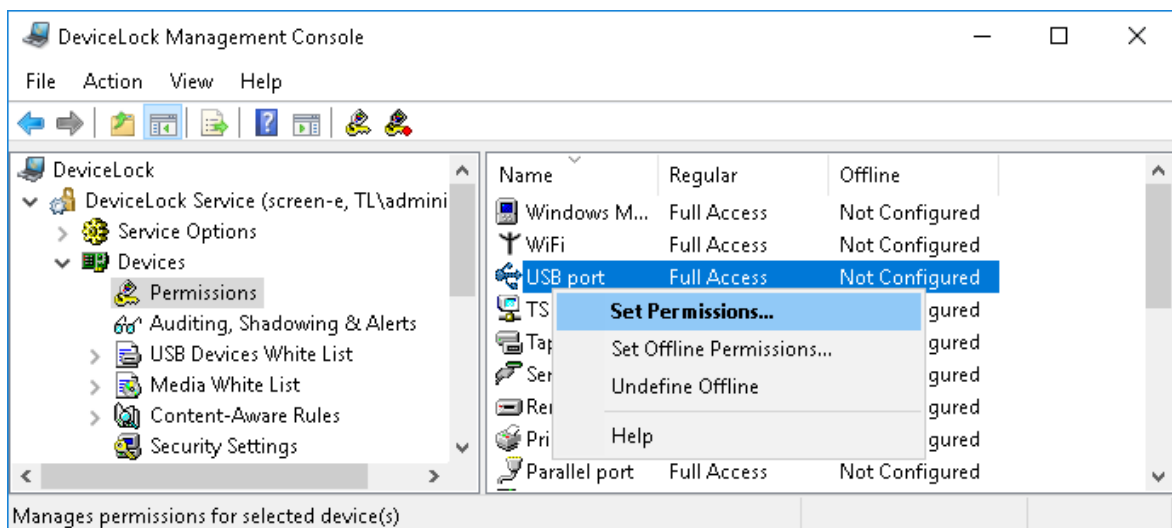
7. Select the device model's record in the **USB Devices Database** list, and then click the **Add** button below this list.

If you do not have devices in the **USB Devices Database** list, click the **USB Devices Database** button below this list, and then add devices as described in the [USB Devices Database](#) section of this manual. When you finished adding devices to the database, click **OK** to save this database and close the **USB Devices Database** dialog box.

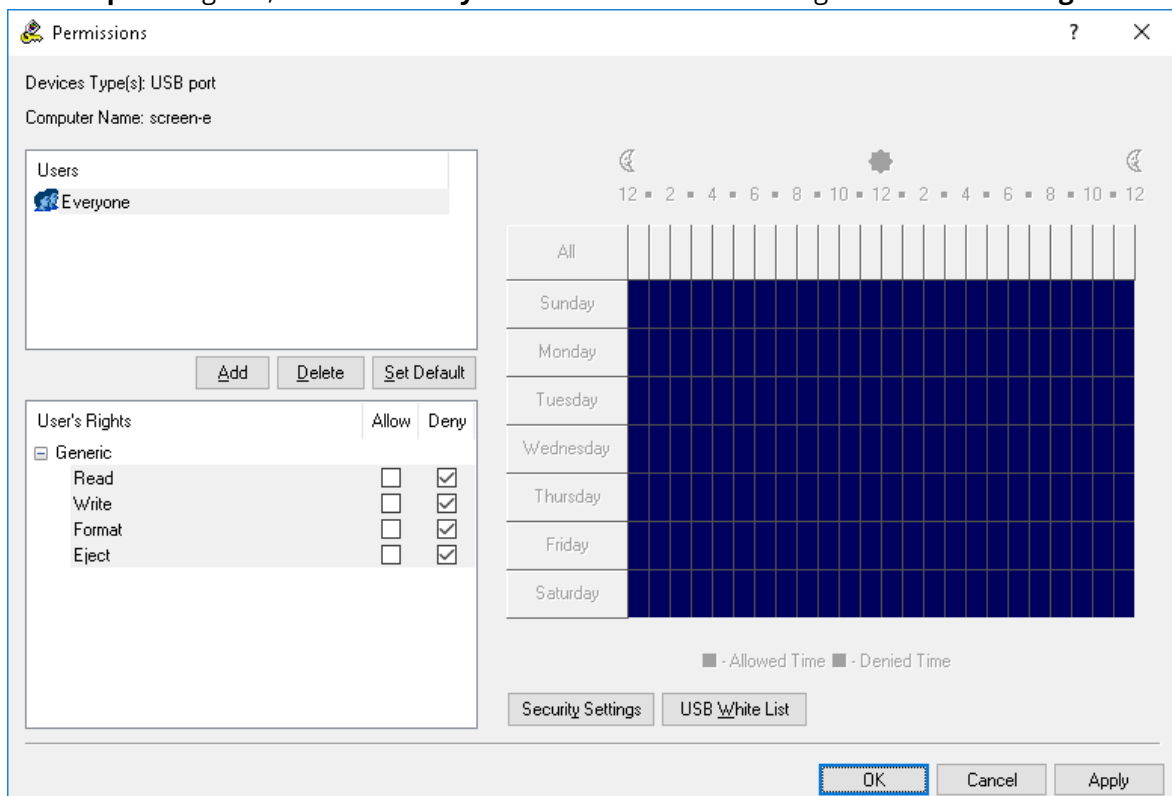
8. Click **OK** to apply the white list settings and close the **USB Devices White List** dialog box, click **OK** to apply changes and close the **Permissions** dialog box, and then click **Yes** to confirm that you really want to deny all users access to the USB port.

***For all users all USB devices are denied except the mouse and keyboard but the Administrators group can use a certain unique USB storage device:***

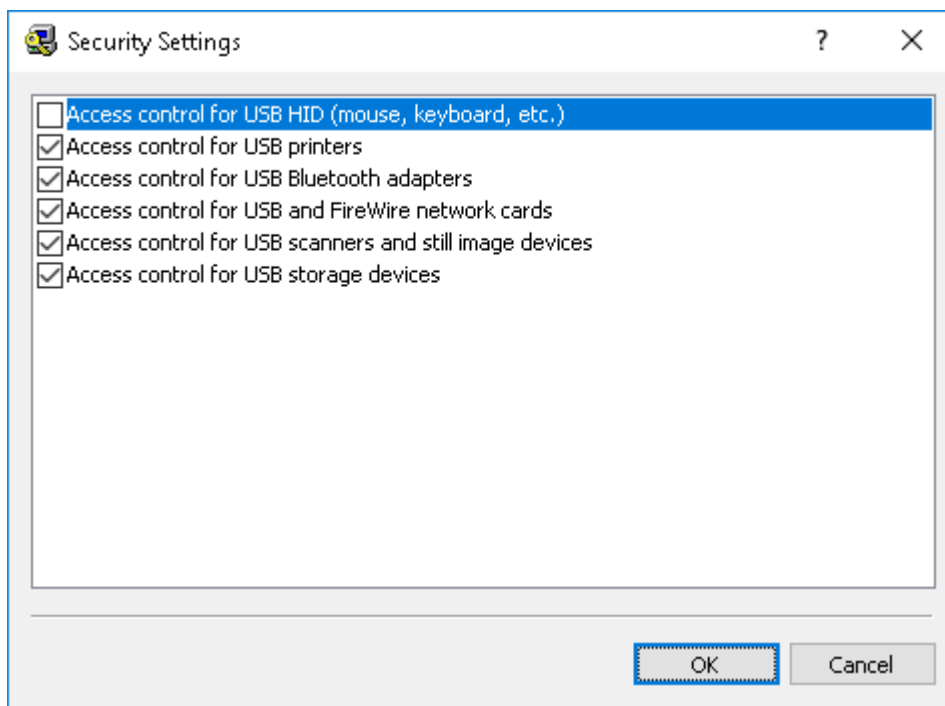
1. Select the **USB port** record from the list of device types under **Permissions**, and then select **Set Permissions** from the shortcut menu available by a right mouse click.



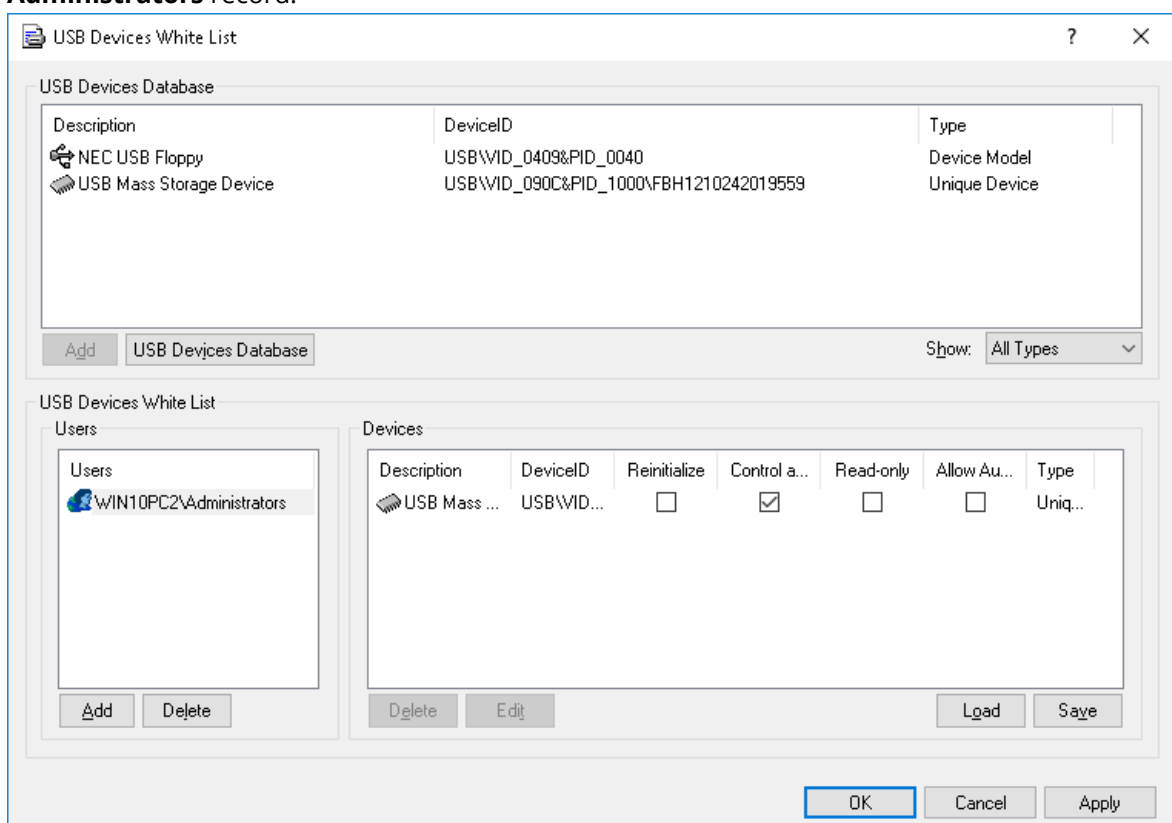
- Click the **Add** button in the **Permissions** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.



- Click the **Security Settings** button in the **Permissions** dialog box, and then clear the **Access control for USB HID (mouse, keyboard, etc.)** check box.



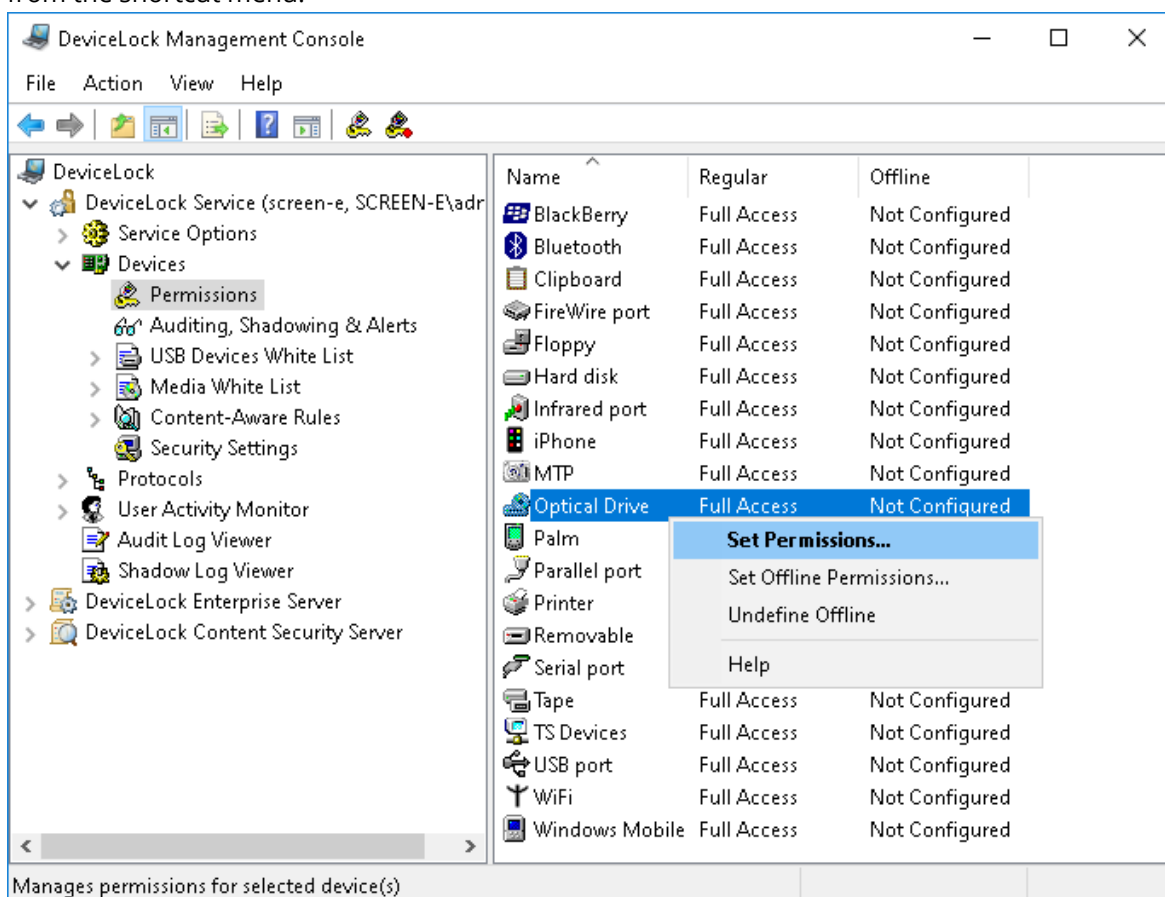
- Click **OK** to close the **Security Settings** dialog box
- Click the **USB White List** button in the **Permissions** dialog box.
- In the **USB Devices White List** dialog box that appears, click the **Add** button below the **Users** list and add the **Administrators** group (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, and then select the **Administrators** record.



7. Select the unique device's record in the **USB Devices Database** list, and then click the **Add** button below this list.  
If you do not have devices in the **USB Devices Database** list, click the **USB Devices Database** button below this list, and then add devices as described in the [USB Devices Database](#) section of this manual. When you finish adding devices to the database, click **OK** to save this database and close the **USB Devices Database** dialog box.
8. Click **OK** to apply the white list settings and close the **USB Devices White List** dialog box, click **OK** to apply changes and close the **Permissions** dialog box, and then click **Yes** to confirm that you really want to deny all users access to the USB port.

***For all users all CD/DVD/BD drives are read-only but the Administrators group can burn (write) CD/DVD/BD discs:***

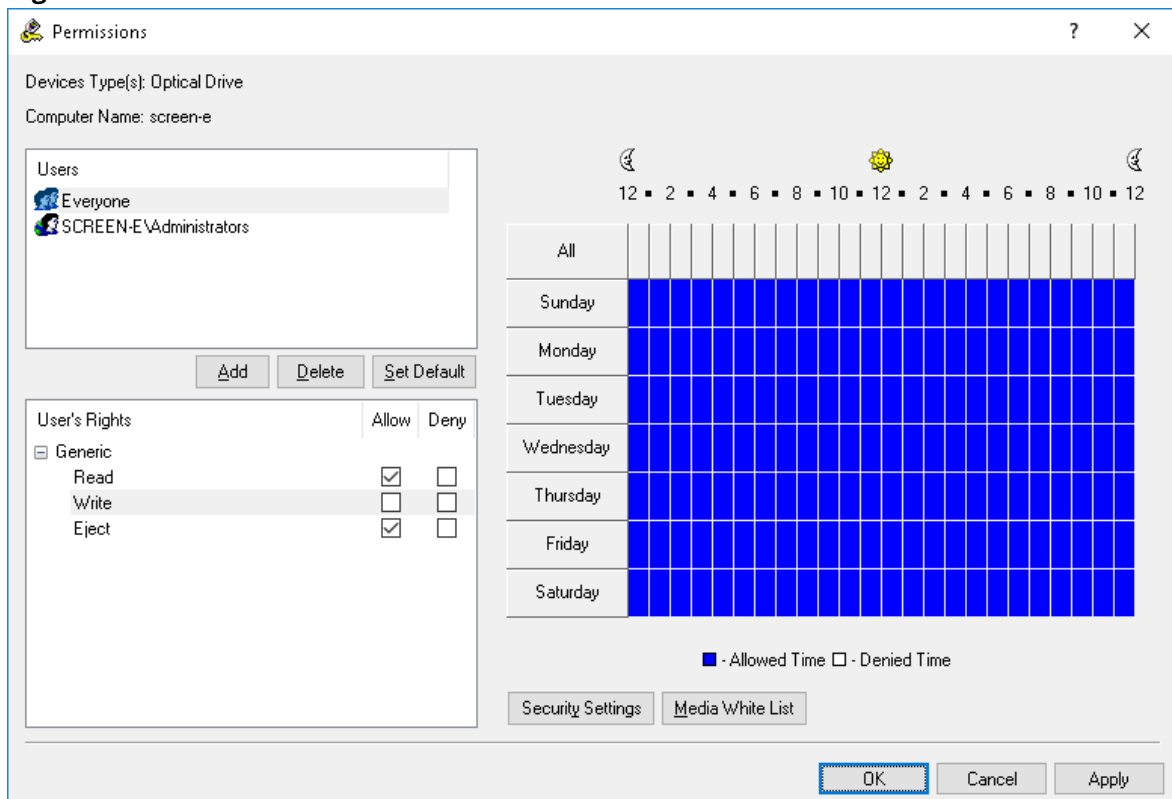
1. Select the **Optical Drive** device type in the **Permissions** node, and then select **Set Permissions** from the shortcut menu.



2. Click the **Add** button in the **Permissions** dialog box and add the **Administrators** group (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Administrators** record and enable all rights in the **User's Rights** list.
3. Click the **Add** button in the **Permissions** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box. Select the **Everyone** record and disable the **Write** right in the **User's**



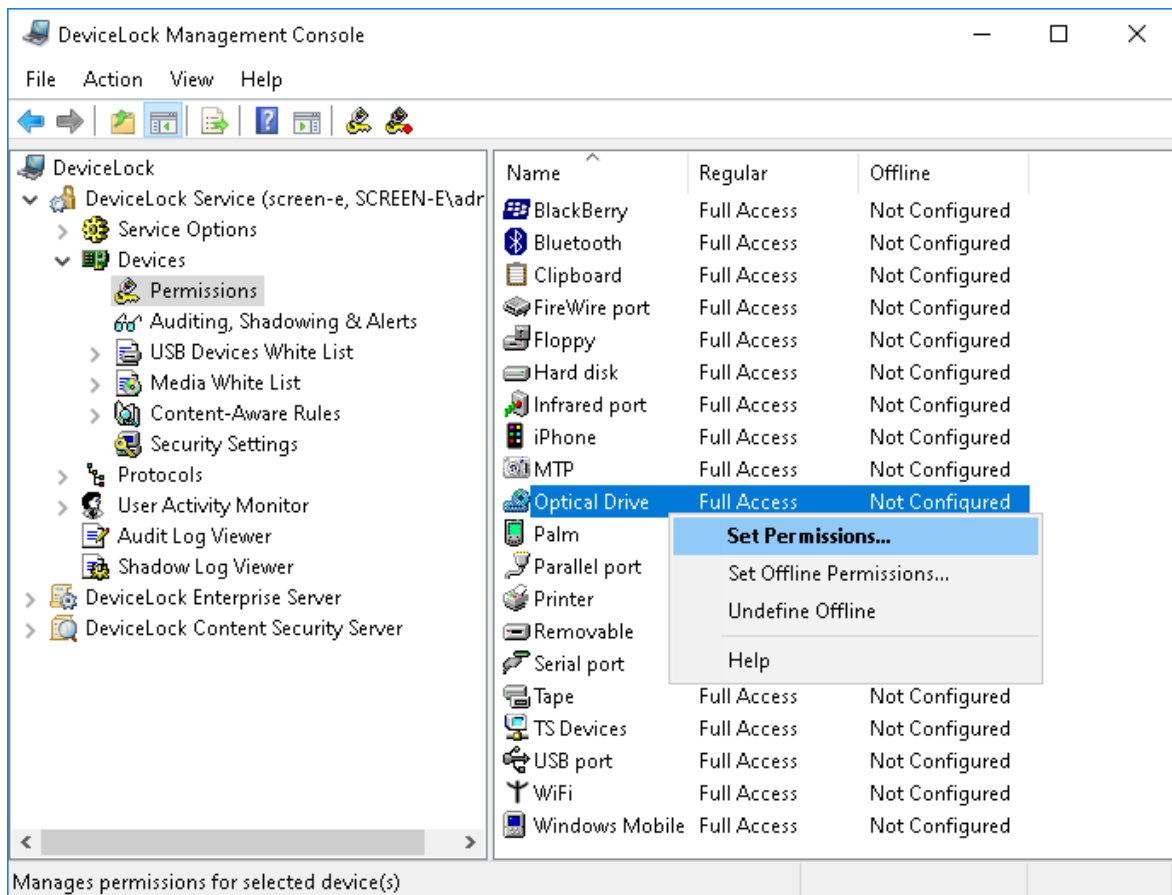
## Rights list.



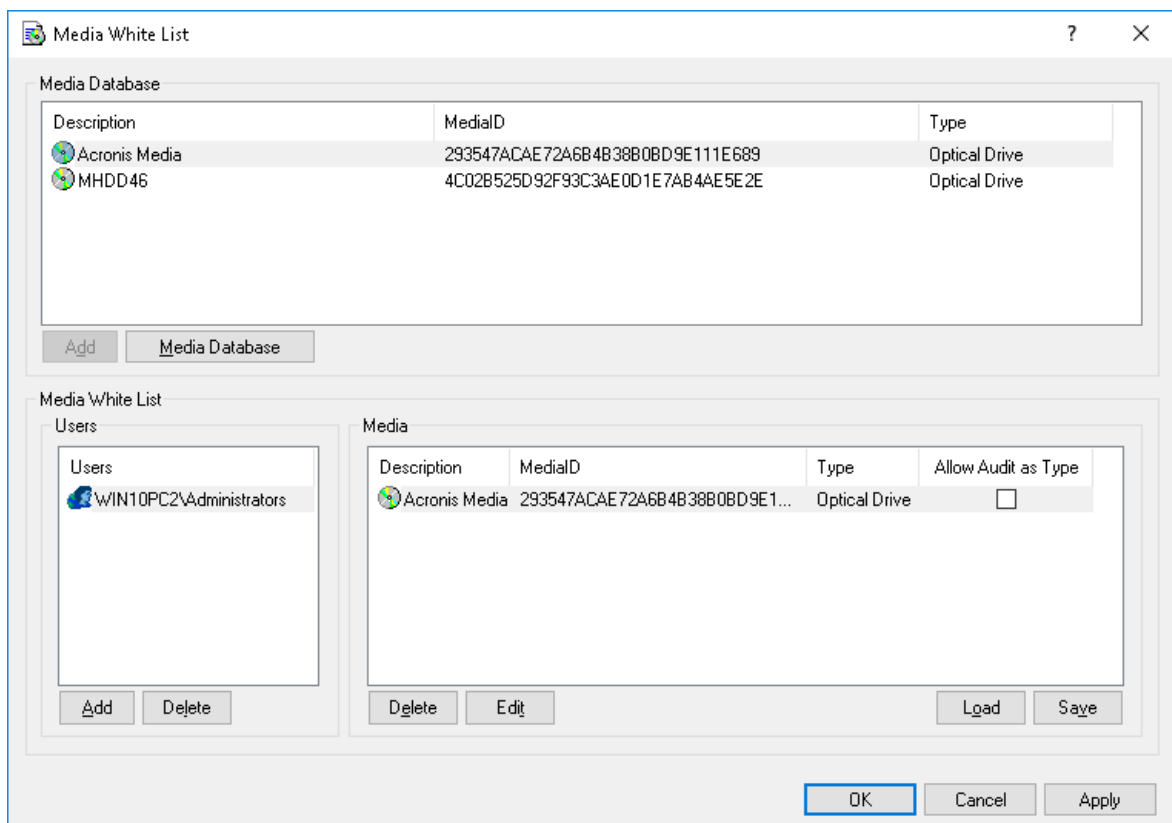
4. Click **OK** to apply changes and close the **Permissions** dialog box.

***For all users all CD/DVD/BD drives are denied but the Administrators group can read a certain optical disc:***

1. Select the **Optical Drive** device type in the **Permissions** node, and then select **Set Permissions** from the shortcut menu available by a right mouse click.



- Click the **Add** button in the **Permissions** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and disable all rights in the **User's Rights** list.
- Click the **Media White List** button in the **Permissions** dialog box.
- In the **Media White List** dialog box that appears, click the **Add** button below the **Users** list and add the **Administrators** group (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, and then select the **Administrators** record.

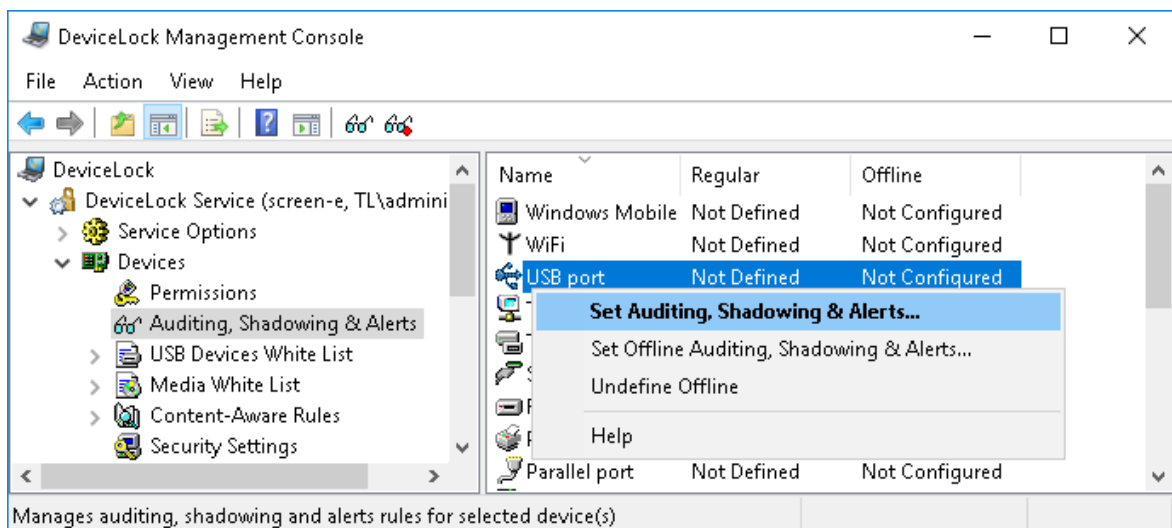


5. Select the media's record in the **Media Database** list, and then click the **Add** button below this list.  
If you do not have records in the **Media Database** list, click the **Media Database** button below this list, and then authorize a media as described in the [Media Database](#) section of this manual. When you finish authorizing a media, click **OK** to save the database and close the **Media Database** dialog box.
6. Click **OK** to apply the white list settings and close the **Media White List** dialog box. Click **OK** to apply changes and close the **Permissions** dialog box. Then click **Yes** to confirm that you really want to deny access to CD/DVD/BD drives for all users.

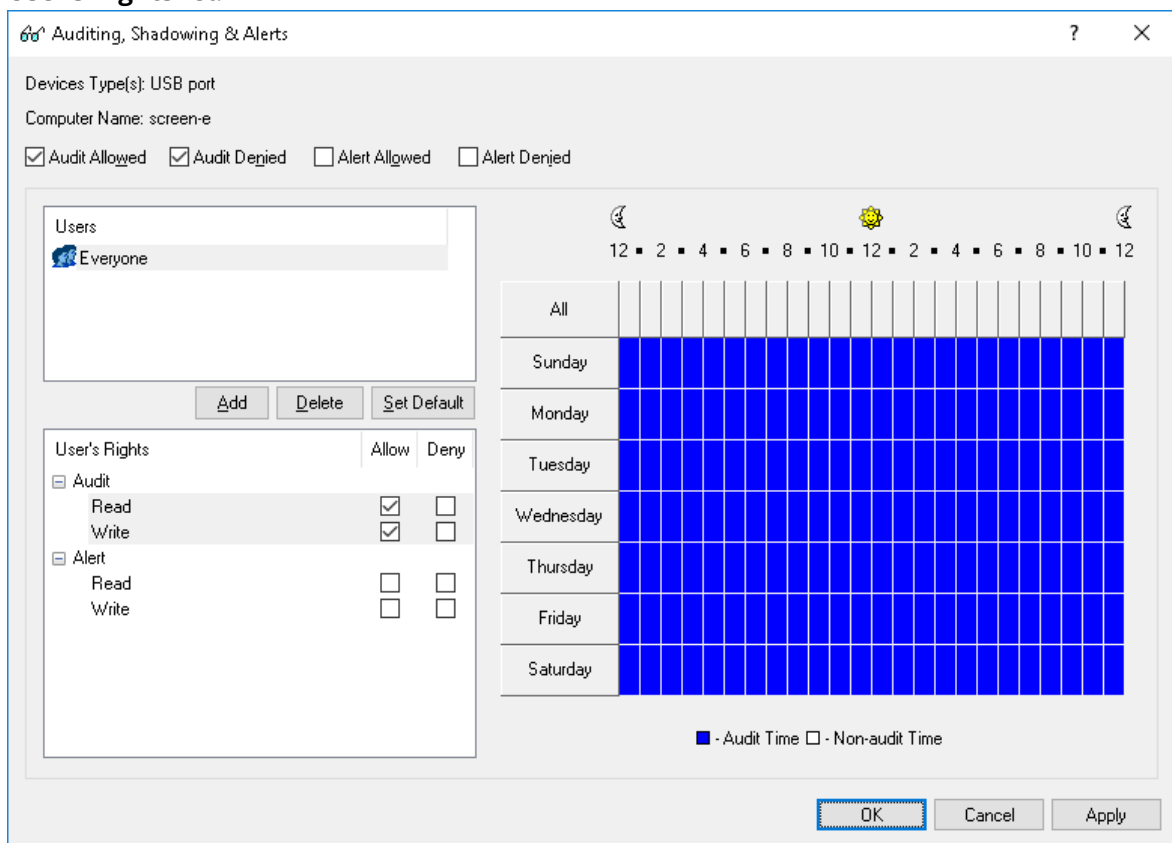
## Audit & Shadowing Examples

### ***Log insert, remove and access actions for any USB devices for all users:***

1. Select the **USB port** record from the list of device types under **Auditing, Shadowing & Alerts**, and then select **Set Auditing, Shadowing & Alerts** from the shortcut menu available by a right mouse click.



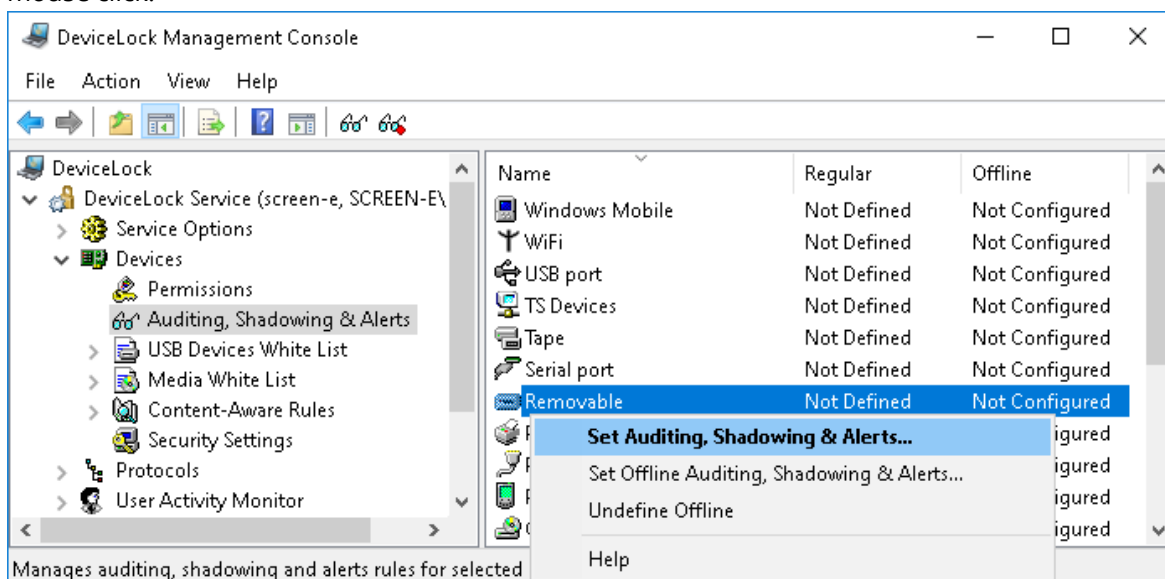
- Click the **Add** button in the **Audit** dialog box and add the **Everyone** user (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Everyone** record and enable **Read** and **Write** audit rights in the **User's Rights** list.



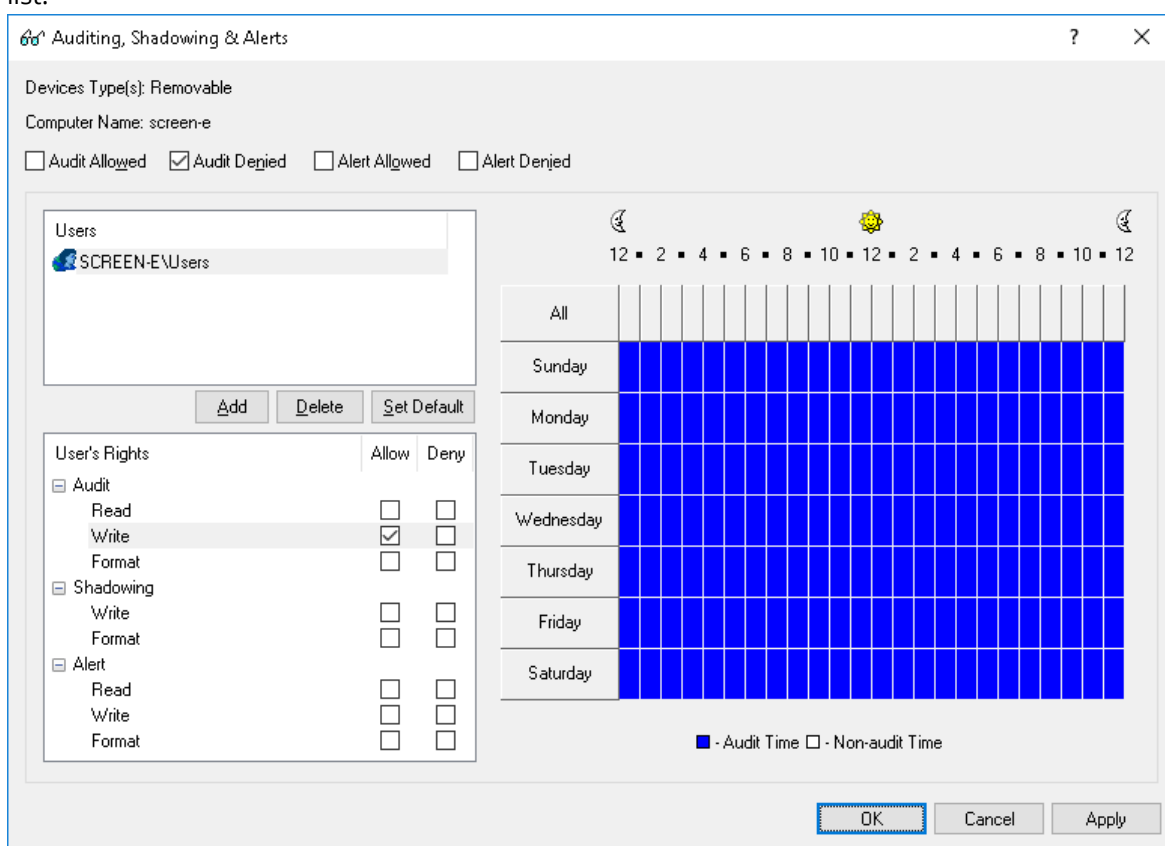
- Select the **Audit Allowed** and **Audit Denied** check box at the top of the **Audit** dialog box, and then click **OK** to apply changes and close the **Auditing, Shadowing & Alerts** dialog box.

**Log only file and folder names upon denied write attempts for removable storage devices for the Users group:**

1. Select the **Removable** record from the list of device types under **Auditing, Shadowing & Alerts**, and then select **Set Auditing, Shadowing & Alerts** from the shortcut menu available by a right mouse click.



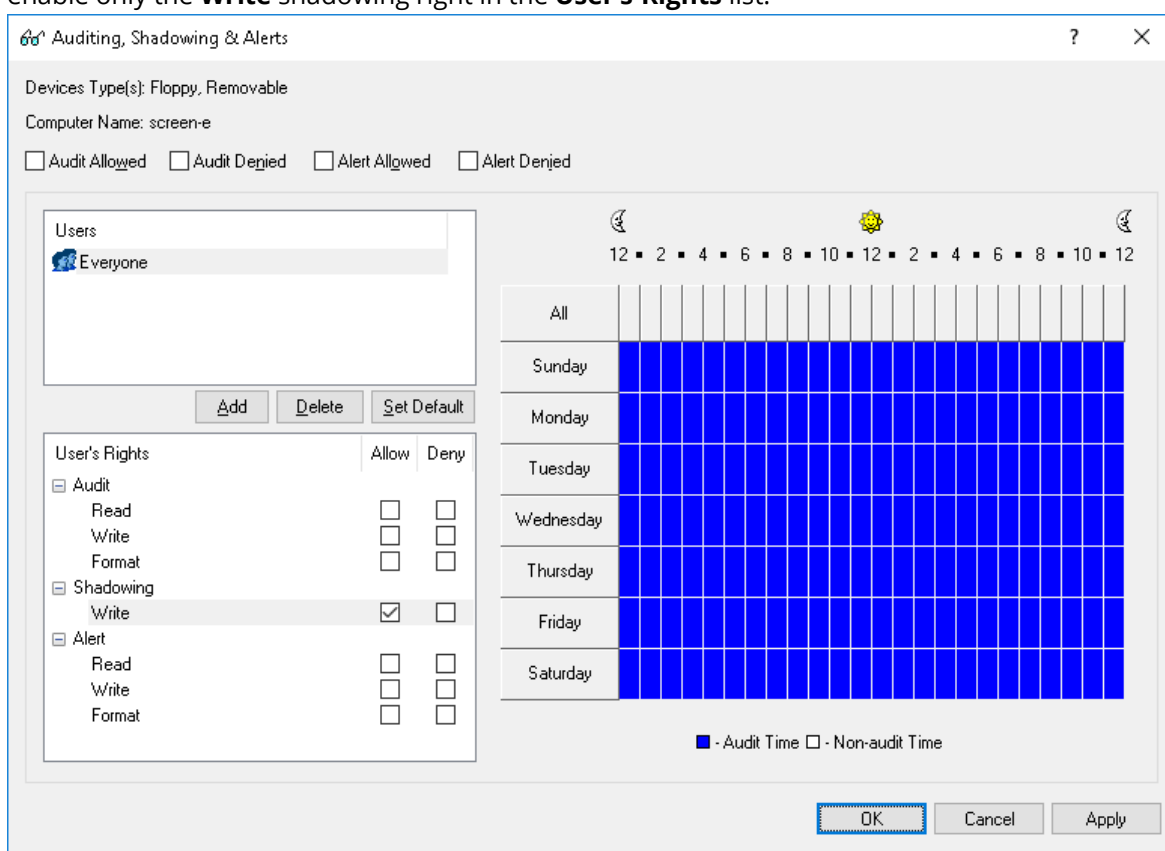
2. Click the **Add** button in the **Audit** dialog box and add the **Users** group (type the name or browse for all available names and select the needed one). Click **OK** to close the **Select Users or Groups** dialog box, select the **Users** record and enable only the **Write** audit right in the **User's Rights** list.



3. Select only the **Audit Denied** check box at the top of the **Audit** dialog, and then click **OK** to apply changes and close the **Auditing, Shadowing & Alerts** dialog box.
4. Enable the **Audit folder operations** parameter under **Auditing & Shadowing** in **Service Options**.

**Shadow all data written to removable storage devices and floppies by any user:**

1. Select **Floppy** and **Removable** records from the list of device types under **Auditing, Shadowing & Alerts**, and then select **Set Auditing, Shadowing & Alerts** from the shortcut menu available by a right mouse click.
2. Click the **Add** button in the **Audit** dialog box and add the **Everyone** user. Click **OK** to close the **Select Users or Groups** dialog box and select the **Everyone** record. Disable all audit rights and enable only the **Write** shadowing right in the **User's Rights** list.



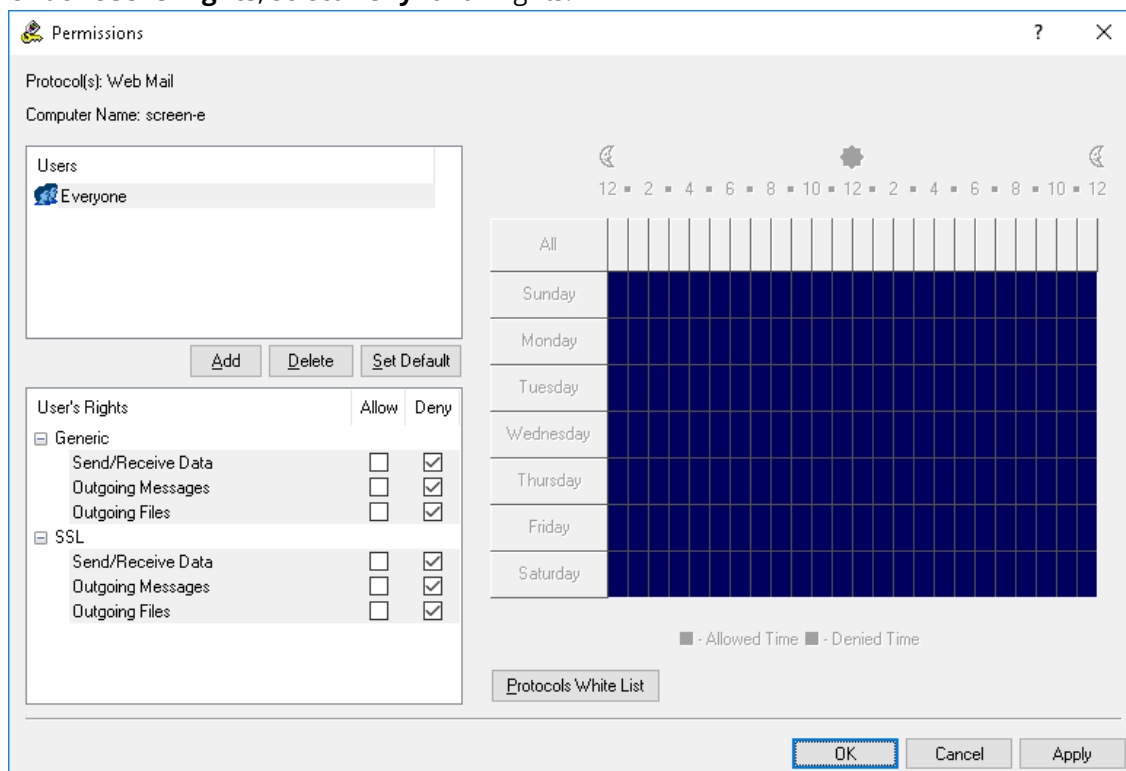
3. Click **OK** to apply changes and close the **Auditing, Shadowing & Alerts** dialog box.

## Permission Examples for Protocols

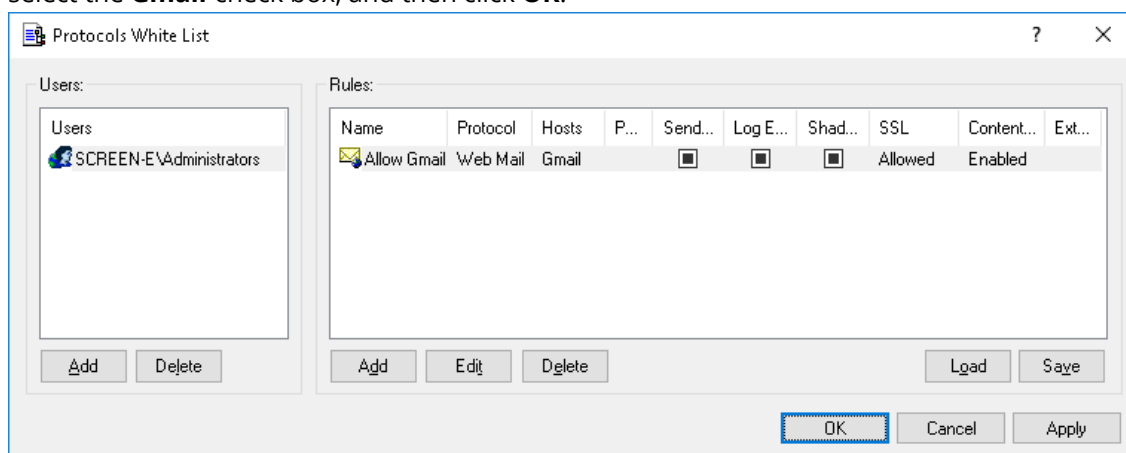
**For all users all Webmail services are denied, but the Administrators group can access Gmail:**

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, select **Permissions**.
3. In the details pane, right-click **Web Mail**, and then click **Set Permissions**.

4. In the **Permissions** dialog box, do the following:
  - a. Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.
  - b. Under **Users**, select **Everyone**.
  - c. Under **User's Rights**, select **Deny** for all rights.



- d. Click **Protocols White List**.
5. In the **Protocols White List** dialog box, do the following:
  - a. Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Administrators**, and then click **OK**.
  - b. Under **Users**, select **Administrators**, and then, under **Rules**, click **Add**. In the **Add Rule** dialog box, in the **Description** box, specify the rule name. Next, under **Web Mail services**, select the **Gmail** check box, and then click **OK**.



- c. Click **OK** or **Apply** to apply the white list settings and close the **Protocols White List** dialog box.
6. In the **Permissions** dialog box, click **OK** or **Apply**.

**The FileSharing Trusted Users group is allowed to use Windows-based applications for Dropbox and Yandex.Disk as well as the Backup and Sync from Google application (formerly Google Drive Sync):**

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, right-click **White List**, and then click **Manage**.
3. In the **Protocols White List** dialog box, do the following:
  - a. Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **FileSharing Trusted Users**, and then click **OK**.
  - b. Under **Users**, select **FileSharing Trusted Users**, and then, under **Rules**, click **Add**.
4. In the **Add Rule** dialog box, do the following:
  - a. In the **Protocol** list, click **SSL**.
  - b. In the **Name** box, specify the rule name.
  - c. In the **Hosts** box, enter the following server names separated by a comma or semicolon:
    - Dropbox servers:  
\*.dropbox.com; \*.compute-1.amazonaws.com
    - Google servers:  
\*accounts.google.com; \*www.googleapis.com
    - Yandex.Disk servers:  
webdav.yandex.ru; \*downloader.disk.yandex.ru; uploader\*.disk.yandex.net;  
push.yandex.ru; \*.storage.yandex.net; oauth.yandex.ru; cloud-api.yandex.net

**Add Rule**

Protocol: **SSL**

Name: **Allow Dropbox, Yandex.Disk, and Backup and Sync from Google**

If this rule triggers

☒ Send Alert ☒ Log Event ☐ Shadow Copy

Hosts:

Example: www.mydomain.com; \*.myhost.net; 12.13.14.15;

\*.dropbox.com; \*.compute-1.amazonaws.com; \*accounts.google.com; \*www.googleapis.com; webdav.yandex.ru; \*downloader.disk.yandex.ru; uploader\*.disk.yandex.net; push.yandex.ru; \*.storage.yandex.net; oauth.yandex.ru; cloud-api.yandex.net

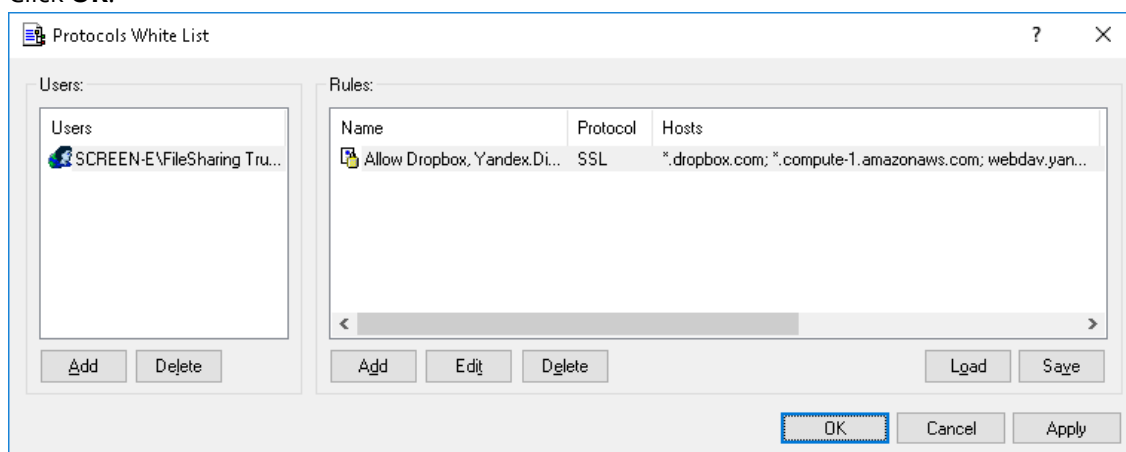
Ports:

Example: 25; 2025-2035

**OK** Cancel



- d. Click **OK**.



5. Click **OK** or **Apply** to apply the white list settings and close the **Protocols White List** dialog box.

### Note

Access control, auditing, shadowing and content inspection will be disabled for all data transfers.

## Content-Aware Rule Examples

***All users are denied the right to copy to devices (Floppy, Removable) and transmit over the network (over HTTP, FTP, SMTP, Web Mail) the following types of content: files containing credit card numbers, password-protected documents and archives, files containing Social Security numbers, and images containing a large amount of text.***

1. In the console tree, expand **DeviceLock Service**, expand **Devices**, right-click **Content-Aware Rules**, and then click **Manage**.
2. In the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Document Properties**.
3. In the **Add Document Properties Group** dialog box, do the following:
  - a. In the **Name** box, specify the name of the group, for example, **Password-protected documents and archives**.
  - b. Select the **Password protected** check box.
  - c. Click **OK**.

*The new content group you created is added to the existing list of content groups under Content Database in the Content-Aware Rules for Devices dialog box. This group will be used to control access to password-protected documents and archives.*
4. In the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Document Properties**.
5. In the **Add Document Properties Group** dialog box, do the following:
  - a. In the **Name** box, specify the name of the group, for example, **Images contain 70% text**.
  - b. Select the **Contains text** check box and specify **70%**.

- c. Click **OK**.

*The new content group you created is added to the existing list of content groups under Content Database in the Content-Aware Rules for Devices dialog box. This group will be used to control access to images containing a large amount of text.*

6. In the **Content-Aware Rules for Devices** dialog box, under **Content Database**, click the drop-down arrow next to **Add Group**, and then click **Complex**.
7. In the **Add Complex Group** dialog box, do the following:
- In the **Name** box, specify the name of the group, for example, **Complex Group 1**.
  - Click **Add**. In the **Content Groups** dialog box, select the following groups: **Credit Card Number, Images, CAD & Drawing, Images contain 70% text, Password-protected documents and archives**, and **US Social Security Number**.  
*You can select these groups simultaneously by holding down the CTRL key while clicking them.*
  - Compose the following logical expression: **US Social Security Number OR Password-protected documents and archives OR Credit Card Number OR Images, CAD & Drawing AND Images contain 70% text**.

NOT	(	Criteria	)	AND/OR
<input type="checkbox"/>		US Social Security Number		OR
<input type="checkbox"/>		Password-protected documents and archives		OR
<input type="checkbox"/>		Credit Card Number		OR
<input type="checkbox"/>		Images, CAD & Drawing		AND
<input type="checkbox"/>		Images contain 70% text		

- d. Click **OK**.

*The new content group you created is added to the existing list of content groups under Content Database in the Content-Aware Rules for Devices dialog box. This group will be used to control access to files containing credit card numbers, password-protected documents and archives, files containing Social Security numbers, and images containing a large amount of text.*

8. In the **Content-Aware Rules for Devices** dialog box, do the following:
  - a. Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.
  - b. Under **Users**, select **Everyone**. Under **Content Database**, select the **Complex Group 1** content group, and then click **Add**.
9. In the **Add Rule** dialog box, do the following:
  - a. Under **Applies to**, select the **Permissions** check box.
  - b. Under **Device Type(s)**, select the **Floppy** and **Removable** check boxes.
  - c. Under **Action(s)**, select the **Deny** check box next to **Write**.

**Add Rule**

Name:

Applies to: ☒ Permissions ☐ Shadowing ☐ Detection

If this rule triggers: ☒ Send Alert ☐ Log Event ☐ Shadow Copy

Devices Type(s):

- ☐ Clipboard
- ☒ Floppy
- ☐ Optical Drive
- ☐ Printer
- ☒ Removable
- ☐ TS Devices

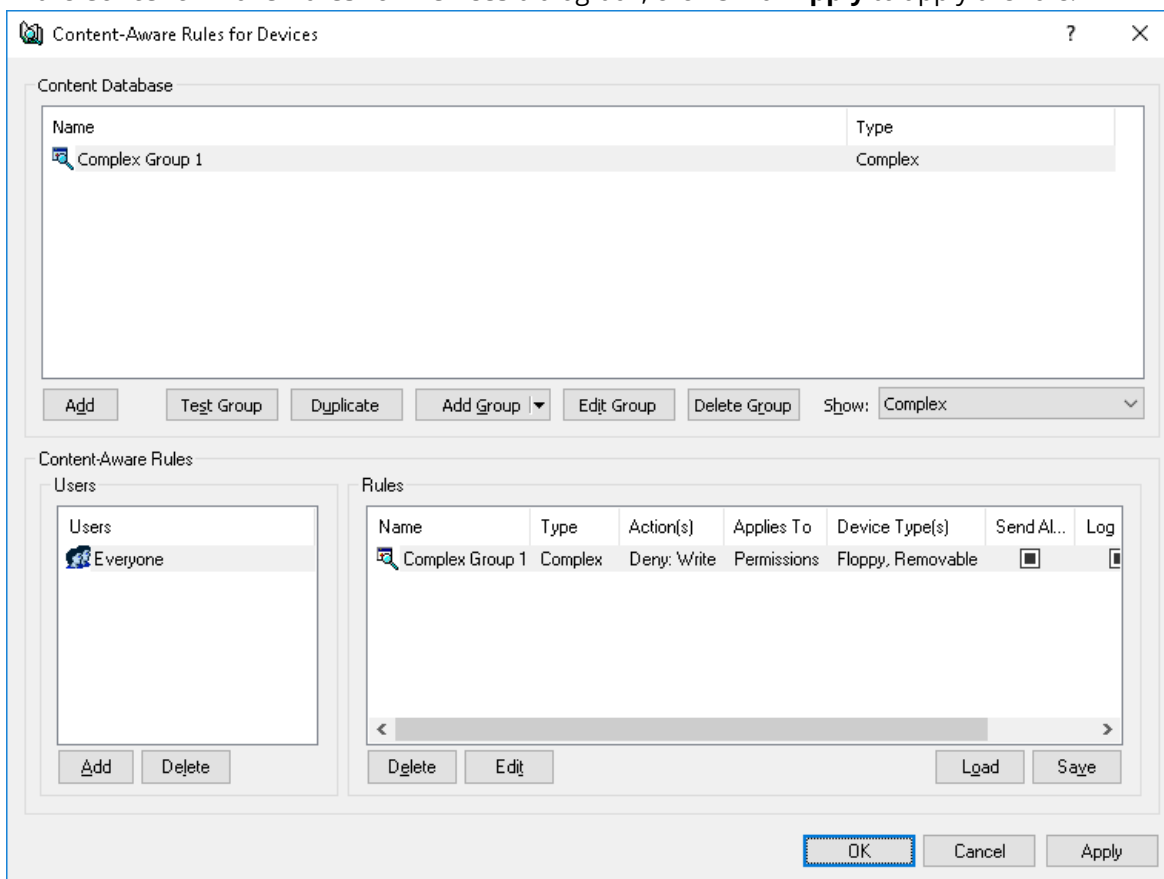
Actions

User's Rights	Allow	Deny
Generic		
Read	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Encrypted		
Read	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>

OK Cancel

- d. Click **OK**.

10. In the **Content-Aware Rules for Devices** dialog box, click **OK** or **Apply** to apply the rule.



11. In the console tree, expand **Protocols**, right-click **Content-Aware Rules**, and then click **Manage**.
12. In the **Content-Aware Rules for Protocols** dialog box, do the following:
- Under **Users**, click **Add**. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.
  - Under **Users**, select **Everyone**. Under **Content Database**, select the **Complex Group 1** content group, and then click **Add**.
13. In the **Add Rule** dialog box, do the following:
- Under **Applies to**, select the **Permissions** check box.
  - Under **Protocol(s)**, select the **FTP**, **HTTP**, **SMTP**, and **Web Mail** check boxes.
  - Under **Action(s)**, select the **Deny** check box next to **Generic: Outgoing Files** and **SSL: Outgoing Files**.

**Add Rule** [?] [X]

Name:

Applies to: ☒ Permissions ☐ Shadowing ☐ Detection

If this rule triggers: ☒ Send Alert ☒ Log Event ☒ Shadow Copy

Protocol(s):

<input type="checkbox"/> File Sharing	<input type="checkbox"/> Mail.Ru Agent	<input type="checkbox"/> Yahoo Messenger
<input checked="" type="checkbox"/> FTP	<input type="checkbox"/> MAPI	
<input checked="" type="checkbox"/> HTTP	<input type="checkbox"/> Skype	
<input type="checkbox"/> IBM Notes	<input checked="" type="checkbox"/> SMTP	
<input type="checkbox"/> ICQ/AOL Messenger	<input type="checkbox"/> Social Networks	
<input type="checkbox"/> IRC	<input type="checkbox"/> Viber	
<input type="checkbox"/> Jabber	<input checked="" type="checkbox"/> Web Mail	

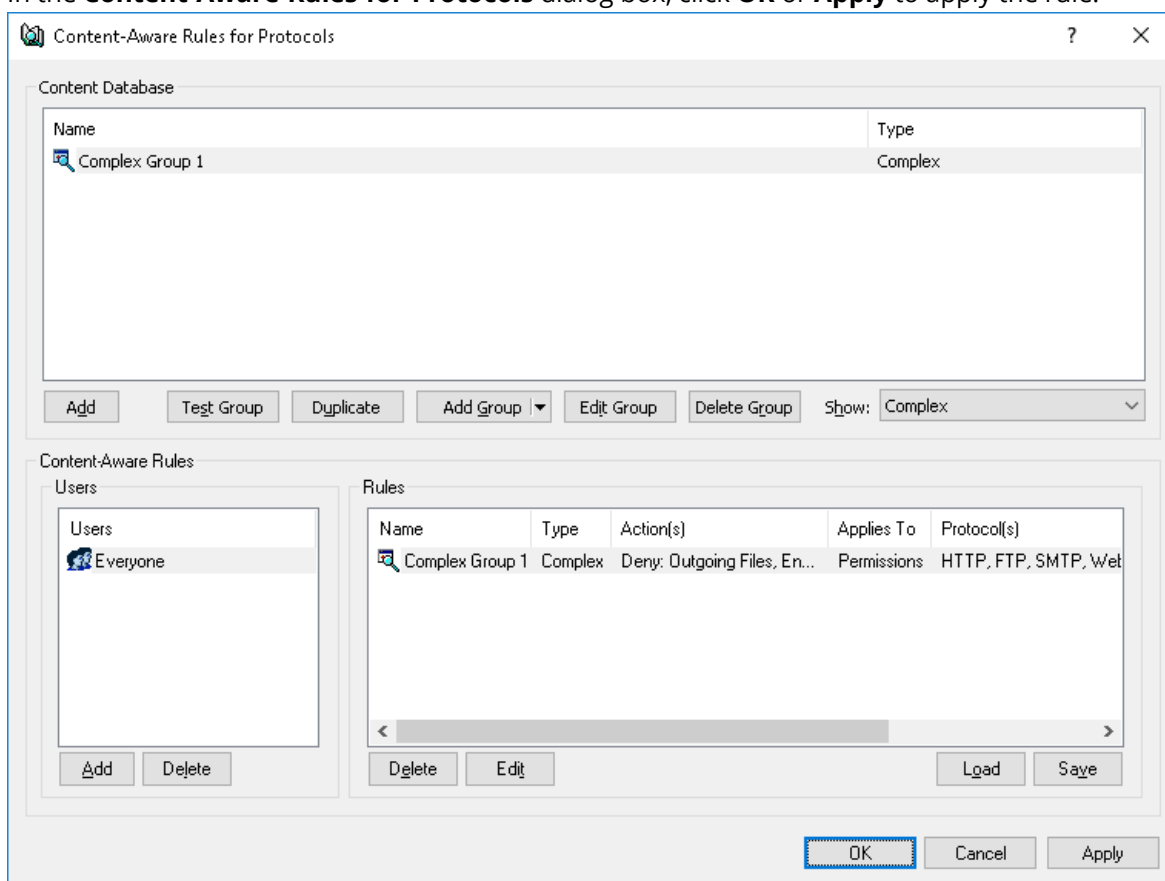
Actions

User's Rights	Allow	Deny
<input checked="" type="checkbox"/> Generic		
POST Requests	<input type="checkbox"/>	<input type="checkbox"/>
Outgoing Messages	<input type="checkbox"/>	<input type="checkbox"/>
Outgoing Files	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> SSL		
POST Requests	<input type="checkbox"/>	<input type="checkbox"/>
Outgoing Messages	<input type="checkbox"/>	<input type="checkbox"/>
Outgoing Files	<input type="checkbox"/>	<input checked="" type="checkbox"/>

OK Cancel

d. Click **OK**.

14. In the **Content-Aware Rules for Protocols** dialog box, click **OK** or **Apply** to apply the rule.



## Basic IP Firewall Rule Examples

These examples show rules that you can create for the IP Firewall.

***The IP firewall is configured to block Remote Desktop connections to the computer where DeviceLock Service is running:***

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Manage**.
3. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.
4. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **SYSTEM**, and then click **OK**.
5. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select **SYSTEM**.
6. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.
7. In the **Add Rule** dialog box, do the following:
  - a. In the **Name** box, specify the name of the firewall rule, for example, **Block RDP**.
  - b. Under **Protocol**, select the **TCP** and **UDP** check boxes.
  - c. Under **Type**, click **Deny**.
  - d. Under **Direction**, select the **Incoming** check box.

- e. In the **Ports** box, type **3389**.
- f. Click **OK**.
8. Click **OK** or **Apply** to apply the firewall rule settings and close the **Basic IP Firewall** dialog box.

***The IP firewall is configured to allow incoming Post Office Protocol version 3 (POP3) connections for the specified user, while all other incoming connections to the computer where DeviceLock Service is running are blocked:***

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Manage**.
3. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.
4. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.
5. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select **Everyone**.
6. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.
7. In the **Add Rule** dialog box, do the following:
  - a. In the **Name** box, specify the name of the firewall rule, for example, **Deny ALL**.
  - b. Under **Protocol**, select the **TCP** and **UDP** check boxes.
  - c. Under **Type**, click **Deny**.
  - d. Under **Direction**, select the **Incoming** check box.
  - e. In the **Ports** box, type 0-65535.
  - f. Click **OK**.

*The rule you created is displayed under Rules in the right pane of the Basic IP Firewall dialog box.  
This rule will be used to block all remote connections to the client computer.*
8. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.
9. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type the name of the user who is allowed to use POP3, and then click **OK**.
10. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select the user who is allowed to use POP3.
11. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.
12. In the **Add Rule** dialog box, do the following:
  - a. In the **Name** box, specify the name of the firewall rule, for example, **Allow POP3 connections**.
  - b. Under **Protocol**, select the **TCP** check box.
  - c. Under **Type**, click **Allow**.
  - d. Under **Direction**, select the **Incoming** check box.
  - e. In the **Ports** box, type 110.
  - f. Click **OK**.

*The rule you created is displayed under Rules in the right pane of the Basic IP Firewall dialog box.  
This rule will be used to unblock port 110 in the firewall to allow incoming POP3 connections for the specified user.*
13. Click **OK** or **Apply** to apply the firewall rule settings and close the **Basic IP Firewall** dialog box.

***The IP firewall is configured to block all TeamViewer connections to and from the computer where DeviceLock Service is running:***

1. In the console tree, expand **DeviceLock Service**, and then expand **Protocols**.
2. Under **Protocols**, right-click **Basic IP Firewall**, and then click **Manage**.
3. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, click **Add**.
4. In the **Select Users or Groups** dialog box, in the **Enter the object names to select** box, type **Everyone**, and then click **OK**.
5. In the left pane of the **Basic IP Firewall** dialog box, under **Users**, select **Everyone**.
6. In the right pane of the **Basic IP Firewall** dialog box, under **Rules**, click **Add**.
7. In the **Add Rule** dialog box, do the following:
  - a. In the **Name** box, specify the name of the firewall rule, for example, **Deny TeamViewer**.
  - b. Under **Protocol**, select the **TCP** check box.
  - c. Under **Type**, click **Deny**.
  - d. Under **Direction**, select the **Outgoing** check box.
  - e. In the **Ports** box, type 5938.
  - f. Click **OK**.

*The rule you created is displayed under Rules in the right pane of the Basic IP Firewall dialog box.  
This rule will be used to block all TeamViewer connections to its servers.*
8. Click **OK** or **Apply** to apply the firewall rule settings and close the **Basic IP Firewall** dialog box.



# DeviceLock Discovery Overview

## Introducing DeviceLock Discovery

DeviceLock Discovery further extends DeviceLock DLP, helping network administrators and security personnel locating certain types of content stored within and outside the limits of the corporate network. Discovering unwanted content is essential when trying to protect the company's intellectual property, control employee activities and administer computer networks.

DeviceLock Discovery Server is a server component and a part of DeviceLock Content Security Server. DeviceLock Discovery is designed to scan users' workstations and storage systems located inside and outside the company's corporate network, looking for certain types of content according to pre-defined rules. Administrators can assign rules specifying which content is not allowed on the corporate network.

DeviceLock Discovery can audit what types of content are stored on a particular workstation or storage device. Based on the defined security context, this capability allows network administrators and IT security personnel to perform a comprehensive audit regarding the content stored on the organization's premises.

## Understanding DeviceLock Discovery

DeviceLock Discovery is used to discover certain types of content existing on the computers and storage devices connected to the local network. These include supported local synchronization directories for selected cloud storage services. Discovery Agent automatically detects all synchronization folders on computer for selected services and performs scanning and configured Discovery actions for files stored in these folders. When used together with DeviceLock, the DeviceLock Discovery greatly enhances the capabilities of the Content-Aware Rules feature. With DeviceLock Discovery, you can not only locate information, but perform a number of actions to grant or deny access to information, alert the administrator, remove or encrypt discovered content or notify the computer user.

DeviceLock Discovery discovers information based on real file types, and allows using regular expression patterns with numerical conditions and Boolean combinations of matching criteria and keywords. Recognizing more than eighty file formats and data types, DeviceLock Discovery extracts and filters the content of data stored on computers' local hard drives, plug-n-play storage devices and NAS servers attached to the local area network. With DeviceLock Discovery, you can also narrow the search to filter information down to just those pieces meaningful to security auditing, incident investigations and forensic analysis.

## Features and Benefits

The key features and benefits of DeviceLock Discovery are as follows:

**Content-based discovery.** You can discover information and automatically take pre-defined actions based on real type of information as determined by its actual content. Content-based discovery can locate many types of data even if the files are renamed and their extensions changed. Thus, you can identify sensitive content receiving an immediate alert, removing the content on the spot or changing available access rights.

**Document classification-based discovery.** You can discover documents and automatically take pre-defined actions based on:

- Digital fingerprints of sensitive documents being taken and stored on the DeviceLock Enterprise Server. Fingerprint-based discovery can identify full copies as well as pieces of documents, even if the document has been changed.
- Classification labels for third-party products, such as the Boldon James Classifier applications, in which document attributes are set according to the level of sensitivity of the document.

**Document discovery in Elasticsearch.** You can discover documents of interest in Elasticsearch - a distributed system that provides real-time indexing and search for a wide variety of data types. DeviceLock Discovery requests a document search in Elasticsearch, matches search results to discovery rules, and then sends alerts, logs events, and generates reports upon discovery results.

**Expansive coverage of multiple file formats and data types.** You can identify content in the following file formats and data types: Adobe Acrobat (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (\*.pdf), Adobe Framemaker MIF (\*.mif), Ami Pro (\*.sam), Ansi Text (\*.txt), ASCII Text, ASF media files (metadata only) (\*.asf), AutoCAD (\*.dwg, \*.dxf), CSV (Comma-separated values) (\*.csv), DBF (\*.dbf), EBCDIC, EML (emails saved by Outlook Express) (\*.eml), Enhanced Metafile Format (\*.emf), Eudora MBX message files (\*.mbx), Flash (\*.swf), GZIP (\*.gz), HTML (\*.htm, \*.html), iCalendar (\*.ics), Ichitaro (versions 5 and later) (\*.jtd, \*.jbt), JPEG (\*.jpg), Lotus 1-2-3 (\*.123, \*.wk?), MBOX email archives such as Thunderbird (\*.mbx), MHT archives (HTML archives saved by Internet Explorer) (\*.mht), MIME messages (including attachments), MSG (emails saved by Outlook) (\*.msg), Microsoft Access MDB files (\*.mdb, \*.accdb, including Access 2007 and Access 2010), Microsoft Document Imaging (\*.mdi), Microsoft Excel (\*.xls), Microsoft Excel 2003 XML (\*.xml), Microsoft Excel 2007, 2010, and 2013 (\*.xlsx), Microsoft OneNote 2007, 2010, and 2013 (\*.one), Microsoft Outlook data files (\*.PST), Microsoft Outlook/Exchange Messages, Notes, Contacts, Appointments, and Tasks, Microsoft Outlook Express 5 and 6 (\*.dbx) message stores, Microsoft PowerPoint (\*.ppt), Microsoft PowerPoint 2007, 2010, and 2013 (\*.pptx), Microsoft Rich Text Format (\*.rtf), Microsoft Searchable Tiff (\*.tiff), Microsoft Visio (\*.vsd, \*.vst, \*.vss, \*.vdw, \*.vsdx, \*.vssx, \*.vstx, \*.vsdm, \*.vssm, \*.vstm), Microsoft Word for DOS (\*.doc), Microsoft Word for Windows (\*.doc), Microsoft Word 2003 XML (\*.xml), Microsoft Word 2007, 2010, and 2013 (\*.docx), Microsoft Works (\*.wks), MP3 (metadata only) (\*.mp3), Multimate Advantage II (\*.dxx), Multimate version 4 (\*.doc), OpenOffice versions 1, 2, and 3 documents, spreadsheets, and presentations (\*.sxm, \*.sxd, \*.sxi, \*.sxw, \*.sxc, \*.stc, \*.sti, \*.stw, \*.stm, \*.odt, \*.ott, \*.odg, \*.otg, \*.odp, \*.otp, \*.ods, \*.ots, \*.odf) (includes OASIS Open Document Format for Office Applications), Quattro Pro (\*.wb1, \*.wb2, \*.wb3, \*.qpw), QuickTime (\*.mov, \*.m4a, \*.m4v), RAR (\*.rar), TAR (\*.tar), TIFF (metadata only) (\*.tif), TNEF (winmail.dat), Treepad HJT files (\*.hjt), Unicode (UCS16, Mac or Windows byte order, or UTF-8), Visio

XML files (\*.vdx), Windows Metafile Format (\*.wmf), WMA media files (metadata only) (\*.wma), WMV video files (metadata only) (\*.wmv), WordPerfect 4.2 (\*.wpd, \*.wpf), WordPerfect (5.0 and later) (\*.wpd, \*.wpf), WordStar version 1, 2, 3 (\*.ws), WordStar versions 4, 5, 6 (\*.ws), WordStar 2000, Write (\*.wri), XBase (including FoxPro, dBase, and other XBase-compatible formats) (\*.dbf), XML (\*.xml), XML Paper Specification (\*.xps), XSL, XyWrite, ZIP (\*.zip) as well as PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, EMF spooled files and GDI printing (ZjStream).

---

**Note**

Content in AutoCAD (DWG, DXF) file formats can be identified on Windows XP and later systems.

---

**Continuous protection.** You can apply content-based security policies to your entire network periodically with scheduled scans.

**Multiple content detection methods.** You can use multiple methods to identify sensitive content contained in documents (based on regular expressions, keywords, and document properties).

**Centralized content management.** Flexible, content-aware Rules and Actions are managed based on content groups that enable you to centrally define types of content types that you want to control.

**Ability to override access rights.** You can selectively allow or deny access to certain content stored on network computers regardless of preset permissions.

**Inspection of files within archives.** Allows you to perform deep inspection of each individual file contained in an archive. The following inspection algorithm is used: when a compressed archive is detected, all files are extracted from the archive and analyzed individually to detect the content to which to apply the actions defined in Rules and Actions. If the content of at least one file from the archive gets a positive match in the Rules and Actions section, DeviceLock Discovery will apply the corresponding rule or action to the entire archive.

All nested archives are also unpacked and analyzed one by one. Archive files are detected by content, not by extension. The following archive formats are supported: 7z (.7z), ZIP (.zip), GZIP (.gz, .gzip, .tgz), BZIP2 (.bz2, .bzip2, .tbz2, .tbz), TAR (.tar), RAR (.rar), CAB (.cab), ARJ (.arj), Z (.z, .taz), CPIO (.cpio), RPM (.rpm), DEB (.deb), LZH (.lzh, .lha), CHM (.chm, .chw, .hxs), ISO (.iso), UDF (.iso), COMPOUND (.msi), WIM (.wim, .swm), DMG (.dmg), XAR (.xar), HFS (.hfs), NSIS (.exe), XZ (.xz), MslZ (.mslz), VHD (.vhd), FLV (.flv), SWF (.swf) as well as CramFS, SquashFS (.squashfs), NTFS, FAT and MBR file system and disk images. Split (or multi-volume) and password-protected archives are not unpacked.

**Optical Character Recognition (OCR).** The use of the OCR technology allows you to recognize and extract text from scanned documents, camera-captured documents (if these documents were aligned 90 degrees to the camera), and screen shots of documents for further content analysis by Content-Aware Rules.

OCR includes the following capabilities:

- An entire image or some portions of the image can be inverted, rotated, or mirrored.
- Images with poor brightness or low contrast are supported.

- Most fonts can be accurately recognized.

OCR has the following limitations:

- Recognition of handwritten text or any fonts that look like handwritten text is not supported.
- Embossed and engraved texts are not recognized.
- Best recognition results are achieved for black text on a white background.

The built-in OCR supports the following languages: Arabic, Bulgarian, Catalan, Chinese - Simplified, Chinese - Traditional, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, and Turkish. The following image files are supported for OCR processing: BMP files, Dr. Halo CUT files, DDS files, EXR files, Raw Fax G3 files, GIF files, HDR files, ICO files, IFF files (except Maya IFF files), JBIG files, JNG files, JPEG/JIF files, JPEG-2000 files, JPEG-2000 codestream files, KOALA files, Kodak PhotoCD files, MNG files, PCX files, PBM/PGM/PPM files, PFM files, PNG files, Macintosh PICT files, Photoshop PSD files, RAW camera files, Sun RAS files, SGI files, TARGA files, TIFF files, WBMP files, XBM files, and XPM files.

---

**Note**

The OCR feature is only supported on Windows XP and later versions of Windows.

---

**Text in picture detection.** The use of the text-in-picture detection technology allows you to classify all images into two groups: text images (containing text, such as scanned documents or screen shots of documents) and non-text images (those that don't contain text). Timely identifying text images helps prevent or investigate leakage of sensitive information within image files. The following image files are supported: BMP files, Dr. Halo CUT files, DDS files, EXR files, Raw Fax G3 files, GIF files, HDR files, ICO files, IFF files (except Maya IFF files), JBIG files, JNG files, JPEG/JIF files, JPEG-2000 files, JPEG-2000 codestream files, KOALA files, Kodak PhotoCD files, MNG files, PCX files, PBM/PGM/PPM files, PFM files, PNG files, Macintosh PICT files, Photoshop PSD files, RAW camera files, Sun RAS files, SGI files, TARGA files, TIFF files, WBMP files, XBM files, XPM files.

**Inspection of images embedded in documents.** Allows you to perform deep inspection of each individual image embedded in Adobe Portable Document Format (including encrypted files if the type of encryption in the file is one of the following: 40-bit RC4, 128-bit RC4, 128-bit AES and 256-bit AES, and the file permissions do not disable text extraction) (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx). All embedded images are extracted from these documents to the Temp folder of the System user and analyzed independently from text. The text contained inside documents is checked against the list of Rules and Actions that are created based on Keywords, Pattern or Complex content groups. Embedded images are checked against Rules and Actions that are created based on File Type Detection, Document Properties or Complex content groups. The appropriate action will be applied to the entire document if either its text or any of the images contained in the document have a match in the Rules and Actions list.

---

**Note**

Deep inspection of images embedded in files of AutoCAD (DWG, DXF) formats can be performed on Windows XP and later systems only.

---

## How DeviceLock Discovery Works

DeviceLock Discovery can scan remote computers by using one of the three methods.

1. DeviceLock Discovery can scan remote computers via the SMB protocol (network shares).
2. Alternatively, DeviceLock Discovery can perform the scanning via its own lightweight agent (DeviceLock Discovery Agent).
3. Finally, DeviceLock Discovery can scan remote computers by using a lightweight agent built into DeviceLock Service.

Depending upon a particular network configuration and system requirements, administrators may choose one or the other method.

**SMB access** is the easiest to deploy. Requiring neither DeviceLock software installation nor configuration for each local target endpoint, SMB access is a perfect method for remote background scanning of network shares on NAS devices, as well as files servers and other computers running any operating systems including those not directly supported by DeviceLock.



Using the **DeviceLock Discovery Agent** is ideal for scanning computers that have no DeviceLock Service installed. This method will require the deployment of the DeviceLock Discovery Agent throughout all computers to be scanned.



Leveraging the **DeviceLock Service** is a perfect solution for customers already using DeviceLock. As this method uses the existing installations of the DeviceLock Service, no additional deployment is

required. However, this method will only scan Windows-based computers with DeviceLock Service already installed, and will neither be able to scan Mac computers nor computers and networks devices with unsupported operating systems such as NAS devices.

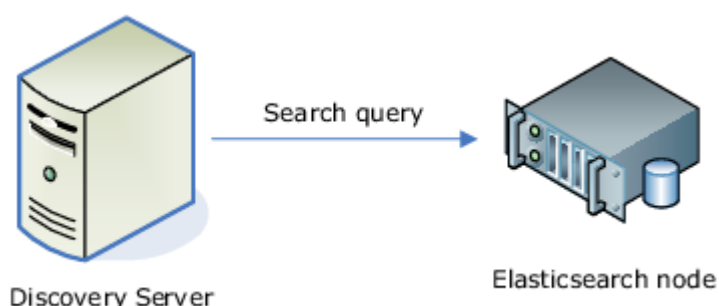


DeviceLock Discovery can be configured to perform certain actions on files being discovered. For example, it can be configured to delete or encrypt a certain file, modify its access rights, send an alert to an administrator, log the event or notify the user of the computer being scanned.

The results and logs are kept in a centralized SQL Server database. An HTML report is generated and kept in the same database. By analyzing the report, administrators can get a clear understanding on search results and review the findings of any content discovered by DeviceLock Discovery. The report is created every time a scanning task finishes.

### ***Discovering documents in Elasticsearch***

DeviceLock Discovery effectively discovers documents of interest in Elasticsearch - a distributed system that provides real-time indexing and search for a wide variety of data types. The Discovery Server requests a document search by the specified configurable parameters, and then applies the discovery rules and actions to documents received from Elasticsearch.



The DeviceLock Discovery agent is not installed on the Elasticsearch node. Discovery is done by direct HTTP access to Elasticsearch nodes. Discovery actions are limited to logging events and sending alerts. The Discovery Server cannot change or delete documents in Elasticsearch.

For further details, see [Elasticsearch Units](#).

## **Scan agent system requirements**

Computers to scan by the DeviceLock Discovery Agent must meet the following requirements:

<b>Operating system</b>	Microsoft Windows XP/Vista/7/8/8.1/10, Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, or Windows Server 2019.  Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
<b>Memory (RAM)</b>	Minimum: 512 MB
<b>Hard disk space</b>	Minimum: 200 MB
<b>Processor</b>	Minimum: Intel Pentium 4

Computers to scan by the DeviceLock Service must meet the following requirements:

<b>Operating system for DeviceLock Service for Windows</b>	Microsoft Windows XP/Vista/7/8/8.1/10, Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, or Windows Server 2019.  Installation is supported on both the 32-bit and the 64-bit editions of the operating system.
<b>Memory (RAM)</b>	Minimum: 512 MB
<b>Hard disk space</b>	Minimum: 400 MB
<b>Processor</b>	Minimum: Intel Pentium 4
<b>Supported virtualization platforms</b>	Microsoft Remote Desktop Services (RDS), Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox, and Windows Virtual PC.

## Licensing

DeviceLock Discovery is licensed separately from DeviceLock DLP.

If you want to use the capabilities of DeviceLock Discovery, you must purchase DeviceLock Discovery licenses. DeviceLock Discovery is licensed on per computer basis. A license is required for each computer or network device scanned with DeviceLock Discovery, regardless of whether the system is set to scan the entire computer or a single folder.

Document discovery in Elasticsearch requires one DeviceLock Discovery license per Elasticsearch index that will be searched for documents. The number of searchable indexes cannot exceed the number of available DeviceLock Discovery licenses.

The trial period for DeviceLock Discovery is 30 days. A maximum of two computers can be scanned with the evaluation version.

# Installing DeviceLock Discovery

To install DeviceLock Discovery, the administrator needs to install the DeviceLock Content Security Server (see [Installing DeviceLock Content Security Server](#)) and provide a license for DeviceLock Discovery (see [Installing DeviceLock Discovery licenses](#) later in this document).

The DeviceLock Management Console is required to administer and use DeviceLock Discovery. For the console installation instructions, see [Installing Management Consoles](#).

## Installing DeviceLock Content Security Server

This section covers the steps to install DeviceLock Content Security Server:

1. [Prepare to Install](#)
2. [Start Installation](#)
3. [Perform Configuration and Complete Installation](#)

### Prepare to Install

Before you install DeviceLock Content Security Server, consider the following:

- The DeviceLock Content Security Server setup program installs two DeviceLock components: Search Server and Discovery Server.
- To install and operate DeviceLock Content Security Server, the following system requirements must be met:

<b>Operating system</b>	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, or Windows Server 2019.  Installation is supported on both 32-bit and 64-bit operating systems.
<b>Database server</b>	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017, or 2019, any edition, including SQL Server Express.  <b>Important</b> Database server is required to run the Search Server and Discovery Server (see <a href="#">Database settings</a> for details).
<b>Hard disk space</b>	Minimum: 1 GB  Recommended: 800 GB (in case of local database server)

- You must have administrator permissions to install DeviceLock Content Security Server.
- For optimal performance and reliability, we recommend that you install DeviceLock Enterprise Server and DeviceLock Content Security Server on different computers.
- There is a special Search Server license which you must purchase for DeviceLock Content Security Server. You can use the same license on an unlimited number of computers running DeviceLock Content Security Server.



Search Server licensing is based on the number of log entries to be indexed for full-text search. Each license allows the indexing of 1,000 entries in the Shadow Log (including shadow copies), 1,000 entries in the UAM log (including keyboard input records), and 5,000 entries in each of the other logs (Audit Log, Deleted Shadow Data Log, Server Log, Monitoring Log, and Policy Log). Depending upon the actual number of log entries on your DeviceLock Enterprise Server/s, you can purchase as many licenses as required. If using several licenses, the Search Server can index as many log entries as the total license count allows. Additional Search Server licenses can be purchased and installed at any time.

The trial period for DeviceLock Content Security Server is 30 days. During the trial period, the Search Server can index 2,000 entries in the Shadow Log, 2,000 entries in the UAM Log, and 10,000 entries in each of the other logs.

- There is a special DeviceLock Discovery license which you must purchase for DeviceLock Content Security Server. A license is required for each computer or network resource scanned with DeviceLock Discovery, regardless of whether you are going to scan the entire computer or a single folder. The trial period for DeviceLock Discovery is 30 days. During this period, DeviceLock Discovery can scan no more than two computers or network resources.
- In case you have several DeviceLock Enterprise Servers on your network, you can also install several DeviceLock Content Security Servers to balance the load.
- When several DeviceLock Content Security Servers are deployed, each Search Server has its own search index. Hence, you have to connect to every DeviceLock Content Security Server and run the same search queries on every Search Server in order to get the complete result set from all the data stored on all DeviceLock Enterprise Servers.
- There are two options for connecting DeviceLock Content Security Server and the database server. Before installing DeviceLock Content Security Server, decide which option best suits your needs:
  1. ONE-TO-ONE - Installing one DeviceLock Content Security Server and connecting it to one database server. This option is most appropriate for small networks (up to several hundred computers).
  2. MANY-TO-MANY - Installing several DeviceLock Content Security Servers and connecting each to its own database server. This option is typical for medium and large networks geographically distributed across a variety of segments.
- We strongly recommend that you exit all Windows programs before you start Setup.

## Start Installation

Use this procedure to begin the installation process.

### **To start installation**

1. Open the archive DeviceLock.zip, and then double-click the file setup\_d1css.exe to start the Setup program.  
*You must run the Setup program on each computer on which you want to install DeviceLock Content Security Server.*

2. Follow the instructions in the Setup program.
3. On the **License Agreement** page, read the License Agreement and then click **I accept the terms in the license agreement** to accept the licensing terms and conditions and proceed with the installation.
4. On the **Customer Information** page, type your user name and organization, and then click **Next**.
5. On the **Destination Folder** page, accept the default installation folder or click **Change** to modify the path as needed. Click **Next**.  
The default installation folder is %ProgramFiles%\DeviceLock Content Security Server on 32-bit Windows or %ProgramFiles(x86)%\DeviceLock Content Security Server on 64-bit Windows.
6. On the **Ready to Install the Program** page, click **Install** to begin the installation.  
*The DeviceLock Content Security Server configuration wizard starts.*  
If you are installing an upgrade or simply reinstalling DeviceLock Content Security Server, and want to keep its current configuration, you do not need to go through the configuration wizard again - just click **Next** and then **Cancel** to close the wizard and keep all existing settings unchanged.  
In case you need to change some parameters but keep others - edit only needed parameters and go through all the configuration wizard's pages up to the **Finish** button on the final page.

---

**Note**

If you are installing Content Security Server for the first time (there are no existing settings on this computer yet) and you cancel the configuration wizard, Setup will not be able to install DeviceLock Content Security Server's service, so you will need to run the configuration wizard again.

---

## Perform Configuration and Complete Installation

The configuration wizard opens automatically during the installation process. This wizard provides the following pages to configure DeviceLock Content Security Server:

- [Service account and connection settings](#)
- [Server administrators and certificate](#)
- [License information](#)
- [Database settings](#)
- [Completing configuration](#)

### Service account and connection settings

On this page, you configure startup options for the DeviceLock Content Security Server service.

DeviceLock Content Security Server

Log on as

☐ Local System account

☒ This account: SCREEN-E\admin Browse...

Password: .....

Confirm password: .....

**NOTE:** We strongly recommend running DeviceLock Content Security Server under an account in the Domain Admins group. DeviceLock Content Security Server must have administrative access to every DeviceLock Enterprise Server that it is trying to connect to.

Connection settings

☒ Dynamic ports

☐ Fixed TCP port:

< Back Next > Cancel

### Log on as

First of all, you should choose an account under which the DeviceLock Content Security Server service will start. As with many other Windows services, the DeviceLock Content Security Server service can start under the special local system account (the SYSTEM user) and on behalf of any user.

To start the service under the SYSTEM user, select the **Local System account** option. Keep in mind that the process working under the SYSTEM user cannot access shared network resources and authenticates on remote computers as an anonymous user. Therefore, DeviceLock Content Security Server configured to run under the SYSTEM user is not able to access DeviceLock Enterprise Server running on the remote computer and it must use DeviceLock Certificate for authentication on it.

For more information about authentication methods, see description of the [Certificate Name](#) parameter.

---

### Important

If the DeviceLock Content Security Server service is configured to run under the Local System account, DeviceLock Discovery Server cannot install or remove DeviceLock Discovery Agents on remote computers.

---

To start the service on behalf of the user, select the **This account** option, enter the user's account name and the password. It is recommended to use a user account that has administrative privileges on all the computers where DeviceLock Enterprise Server is running. Otherwise, you will need to use DeviceLock Certificate authentication.

If you are installing DeviceLock Content Security Server in the domain environment, we recommend that you use a user account that is a member of the Domain Admins group. Since Domain Admins is a member of the local group Administrators on every computer in the domain, members of Domain Admins will have full access to every computer.

Also, consider the following:

- If **Default Security** is disabled on a remote DeviceLock Enterprise Server, the user account specified in the **This account** option must be also in the list of server administrators with at least **Read-only** level of access on that DeviceLock Enterprise Server. Otherwise, the DeviceLock Certificate authentication needs to be used.
- If **Default Security** is disabled on a remote DeviceLock Service, the user account specified in the **This account** option must be also in the list of DeviceLock administrators with at least **Read-only** access rights on that DeviceLock Service. Otherwise, the DeviceLock Certificate authentication should be used or explicit credentials should be specified in the respective DeviceLock Discovery unit.

### **Connection settings**

You can instruct DeviceLock Content Security Server to use a fixed TCP port for communication with the management console, making it easier to configure a firewall. Type the port number in **Fixed TCP port**. To use dynamic ports for RPC communication, select the **Dynamic ports** option. By default, DeviceLock Content Security Server uses port 9134.

Click **Next** to start the DeviceLock Content Security Server service and to proceed to the second page.

### **Starting the Service**

If the current user does not have full administrative access to DeviceLock Content Security Server (in case it already exists and you're installing an upgrade), the configuration wizard will not be able to install the service and apply changes. The following message will appear: "Access is denied." Also, a similar error may occur when the current user does not have local administrative privileges on the computer where DeviceLock Content Security Server is installing.

If you have specified an incorrect user name for the **This account** option or the wrong user password, DeviceLock Content Security Server will not be able to start. The following message will appear: "The account name is invalid or does not exist, or the password is invalid for the account name specified."

You will be notified if the user's account specified for the **This account** option is not a member of the Domain Admins group. The following message will appear: "The account <name> does not belong to the Domain Admins group. Do you want to continue?"

You may continue by clicking **Yes**. However, make sure that either of the following is true.

For Search Server:

- The specified user has administrative access to all remotely running DeviceLock Enterprise Servers  
- OR -
- DeviceLock Certificate (private key) is installed on every computer running DeviceLock Enterprise Server

For DeviceLock Discovery Server:

- The specified user has administrative access to all computers scanned by DeviceLock Discovery Server. This includes computers running DeviceLock Services, DeviceLock Discovery Agents, as well as any computers not having the Agent installed.  
- OR -
- DeviceLock Certificate (public key) is installed on every computer (with DeviceLock Service) scanned by DeviceLock Discovery Server  
- OR -
- Credentials for accessing remote computers are specified in the scanning settings.

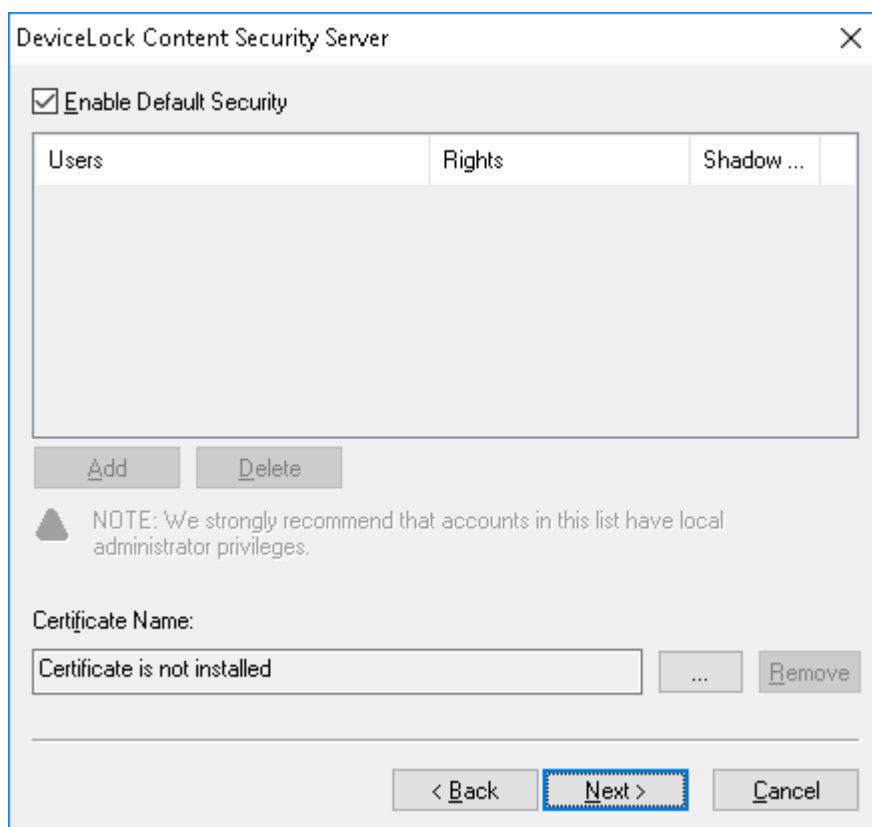
If the user's account specified for the **This account** option does not have the "Log On As A Service" system privilege, the wizard automatically assigns it. This privilege is needed to start the service on behalf of the user. The following message will appear: "The account <name> has been granted the Log On As A Service right."

If all of the service's startup parameters were specified correctly, the wizard starts DeviceLock Content Security Server. The following message will appear: "Please wait while the program is interacting with a service. Starting service DLCSS on Local Computer..."

It takes some time (up to a minute) before the DeviceLock Content Security Server service is started and the next page of the wizard is displayed.

## Server administrators and certificate

On this page of the wizard, you can set up the list of users that have administrative access to DeviceLock Content Security Server, and install DeviceLock Certificate (the private key) if needed.



### ***Enable Default Security***

In the default security configuration all users with local administrator privileges (i.e. members of the local Administrators group) can connect to DeviceLock Content Security Server using a management console, change its settings, run search queries, configure content detection settings, and run discovery tasks.

To turn on the default security, select the **Enable Default Security** check box.

If you need to define more granular access to DeviceLock Content Security Server, turn off the default security by clearing the **Enable Default Security** check box.

Then you need to specify authorized accounts (users and/or groups) that can connect to DeviceLock Content Security Server. To add a new user or group to the list of accounts, click **Add**. You can add several accounts simultaneously.

To delete a record from the list of accounts, use the **Delete** button. Using Ctrl and/or Shift you can highlight and remove several records simultaneously.

To determine the actions allowed to a user or group, select the desired level of access to the server:

- **Full access** - Allows the user or group to install and uninstall DeviceLock Content Security Server, connect to it by using DeviceLock Management Console, and perform any actions on the server, such as: view and change server settings; create and run search queries and tasks; view and change content detection settings; create and run discovery tasks and reports.

- **Change** - Same as full access to the server with the exception of the right to make changes to the list of server administrators or change the level of access to the server for the users or groups already in that list.
- **Read-only** - Allows the user or group to connect to DeviceLock Content Security Server by using DeviceLock Management Console; view server settings; run search queries; view and run existing search tasks; view content detection settings; view discovery reports and manually create new reports based on the existing reports and data already prepared by discovery tasks. This option does not give the right to run discovery tasks, make any changes on the server, or create a new index for the Search Server.

For users and groups with **Change** or **Read-only** access, the **Shadow Data Access** option can be selected to allow access to shadow copies and user activity records. The users and groups with this option selected are allowed to search the content of shadow copies and user activity records, and open, view, and save shadow copies and user activity records from search results.

Without access to shadow data, DeviceLock Content Security Server administrators cannot open, view, or save shadow copies and records of user activity. Search results do not have the **Open**, **Save**, and **View** links, and asterisks are displayed instead of text snippets of shadow copies and user activity records. Logins and passwords in document parameters for user activity records are also replaced with asterisks.

---

### Important

We strongly recommend that DeviceLock Content Security Server administrators be given local administrator rights as installing, updating and uninstalling this server may require access to Windows Service Control Manager (SCM) and shared network resources.

---

### Certificate Name


You may need to deploy the private key to DeviceLock Content Security Server if you want to enable authentication based on DeviceLock Certificate.

There are two methods of DeviceLock Search Server authentication on a remotely running DeviceLock Enterprise Server:

- **User authentication** - The DeviceLock Content Security Server service is running under the user's account that has administrative access to DeviceLock Enterprise Server on the remote computer. For more information on how to run DeviceLock Content Security Server on behalf of the user, please read the description of the [Log on as](#) parameter.
- **DeviceLock Certificate authentication** - In situations where the user under which the DeviceLock Content Security Server service is running cannot access DeviceLock Enterprise Server on the remote computer, you must authenticate based on a DeviceLock Certificate.  
*The same private key should be installed on DeviceLock Enterprise Server and on DeviceLock Content Security Server.*

There are three methods of DeviceLock Discovery Server authentication when scanning a remote computer:

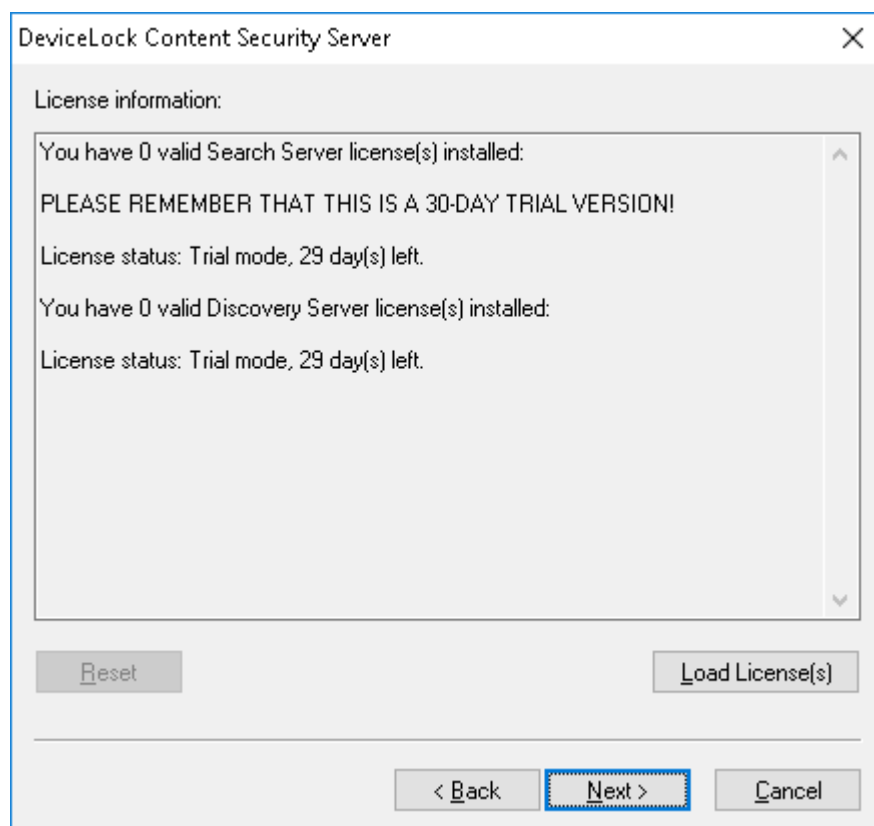
- **User authentication** - The DeviceLock Content Security Server service is running under a certain user account, and these credentials are used to access remote computers being scanned. These credentials will be supplied to either DeviceLock Service, DeviceLock Discovery Agent, or the remote computer if scanning is performed without an agent. For more information on how to run DeviceLock Content Security Server on behalf of a user, please read the description of the [Log on as](#) parameter.
- **Alternative credentials authentication** - The DeviceLock Content Security Server service is running under a user account that has administrative privileges at least on the local computer. DeviceLock Discovery Server will use alternative credentials to log in to remote computer being scanned.
- **DeviceLock Certificate authentication** - Authentication based on a DeviceLock Certificate is used to authenticate on remote computers running DeviceLock Service with the certificate's public key installed.

To install DeviceLock Certificate, click the  button, and select the file containing the certificate's private key. To remove DeviceLock Certificate, click **Remove**.

Click **Next** to apply changes and proceed to the next page of the configuration wizard.

## License information

On this page, you can install your licenses for Search Server and/or DeviceLock Discovery. Search Server and DeviceLock Discovery are licensed separately. The trial period is 30 days.





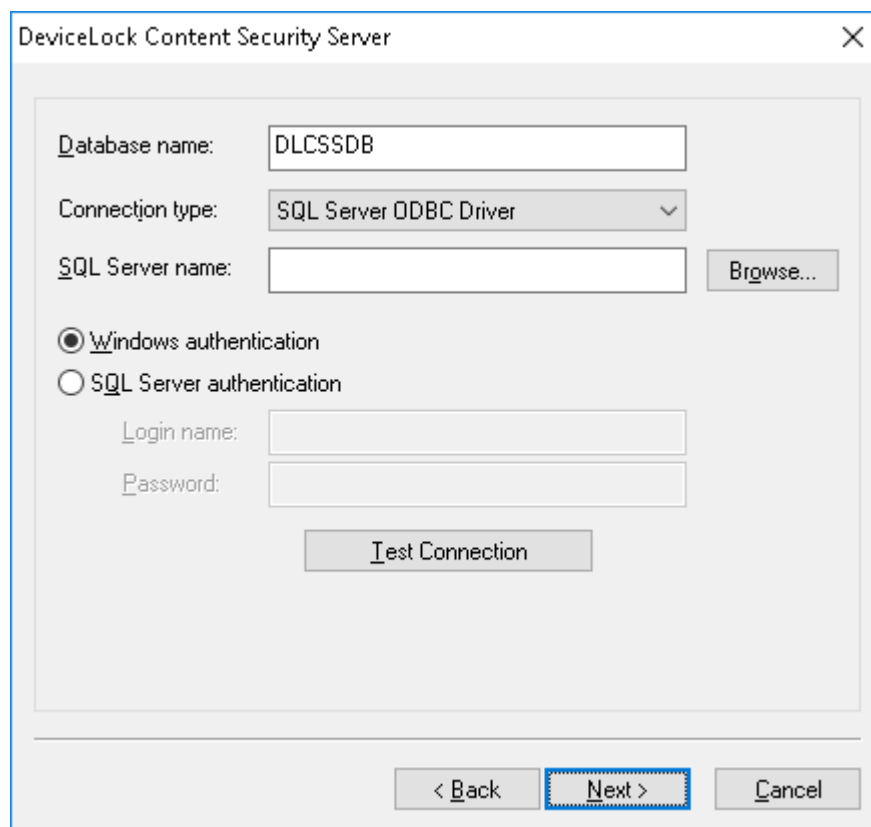
To install a license, click **Load License(s)** and select the license file. You can load several license files in series - one by one. The **License information** box displays summary information about the licenses you're installing.

After Content Security Server has been installed, you can use the DeviceLock Management Console to install a license or view the current license information, including the number of installed licenses and the number of used licenses for Search Server and/or DeviceLock Discovery.

Click **Next** to proceed to configuring the database.

## Database settings

On this page, the wizard prompts you to configure database parameters.



The screenshot shows a window titled "DeviceLock Content Security Server" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Database name:** A text box containing "DLCSSDB".
- Connection type:** A dropdown menu showing "SQL Server ODBC Driver".
- SQL Server name:** A text box with a "Browse..." button to its right.
- Authentication:** Two radio buttons: "Windows authentication" (selected) and "SQL Server authentication".
- Login name:** A text box, visible only if SQL Server authentication is selected.
- Password:** A text box, visible only if SQL Server authentication is selected.
- Test Connection:** A button located below the login and password fields.
- Navigation:** At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

---

### Important

Do not skip this page, as a database is required for the Search Server and Discovery Server to function. Without a database, it is impossible to search using content-aware groups, save and automate search queries, or use the Discovery Server for content discovery.

---

### Database name

In the **Database name** box, view or change the name of the database for DeviceLock Content Security Server. The default name suggested by the wizard is **DLCSSDB**.

---

**Note**

You should not create a database with the specified name manually because the configuration wizard creates the database automatically or uses the existing one.

---

**Connection type**

In the **Connection type** list, you can choose from the following database connection options:

- **SQL Server ODBC Driver** - Connect to Microsoft SQL Server by using an ODBC driver.  
The **SQL Server name** parameter must contain the name of the computer running SQL Server along with the name of the SQL Server instance. A SQL Server name normally consists of two parts: the computer name and the instance name divided by a backslash (such as computer\instance). If the instance name is empty (default instance), the computer name is used as the SQL Server name. To retrieve SQL Server names available on your local network, click the **Browse** button. (You should have access to the remote registry of the SQL Server computer to retrieve the instance name.)

If the **SQL Server name** parameter is empty, it means that SQL Server runs on the same computer as DeviceLock Content Security Server and has the empty (default) instance name.

To connect to SQL Server, authentication parameters must be configured as well.

Select the **Windows authentication** option to authenticate on SQL Server under the account used to run the DeviceLock Content Security Server's service.

If the service runs under the SYSTEM account and SQL Server is on a remote computer, the service will not be able to connect to SQL Server since the SYSTEM account doesn't have the right to access the network. For more information on how to run DeviceLock Content Security Server on behalf of a user, see the description of the [Log on as](#) parameter.

Select the **SQL Server authentication** option to allow SQL Server to perform authentication by checking the login and password previously defined. Before selecting the **SQL Server authentication** option, make sure that your SQL Server is configured for mixed-mode authentication. Enter the SQL Server user name (login) in **Login name** and its password in **Password**.

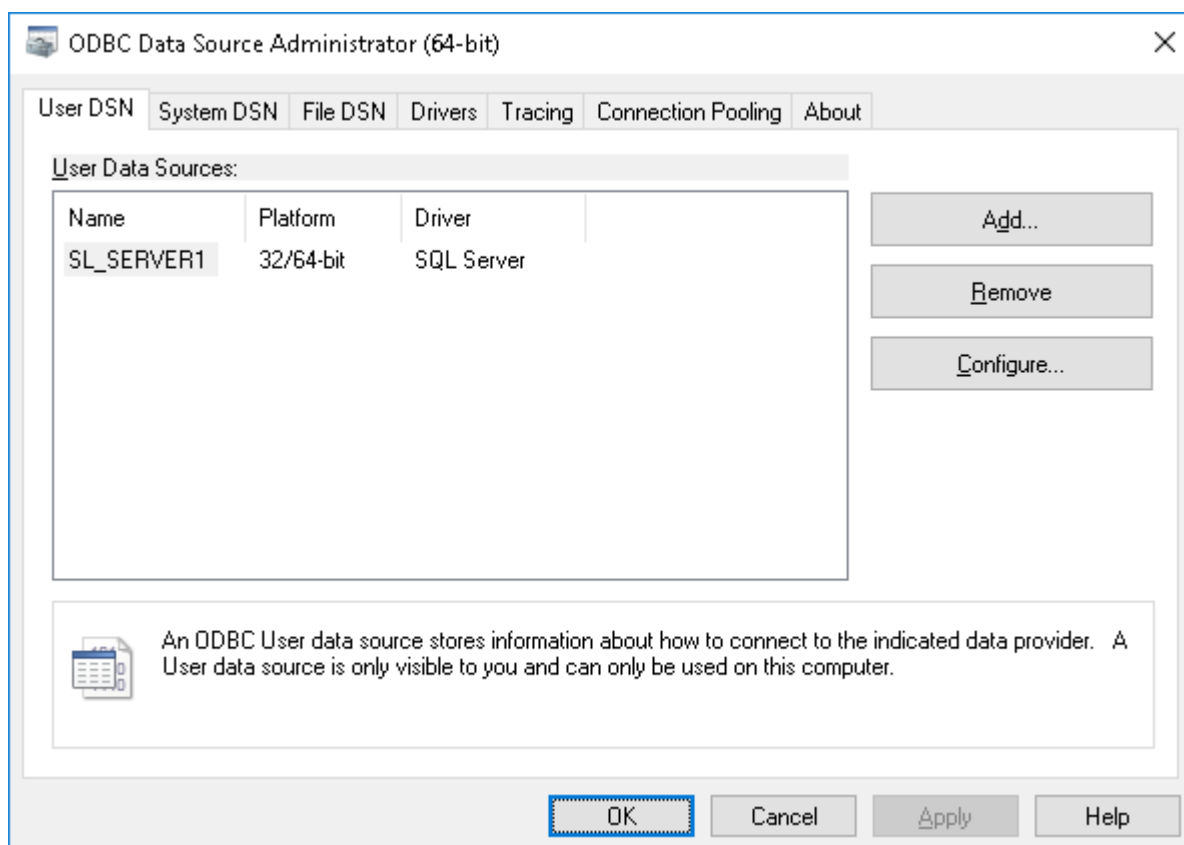
---

**Note**

Windows Authentication is more secure than SQL Server Authentication. When possible, you should use Windows Authentication.

---

- **System Data Source** - Connect to the database server by using a previously created system data source. Select a data source from the **Data Source Name** list.  
To create a data source, use **ODBC Data Source Administrator** from **Control Panel > Administrative Tools**.



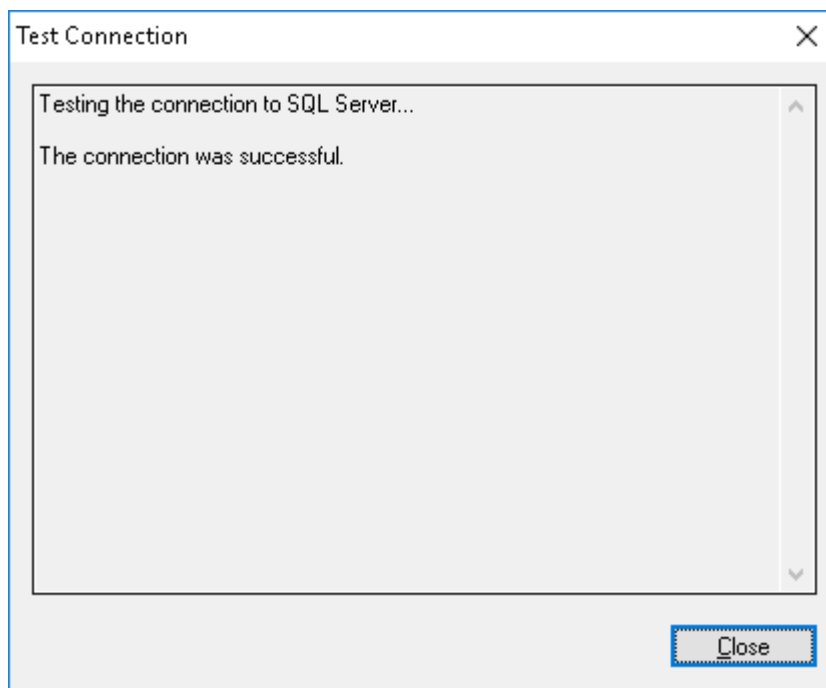
If the data source requires a login name and password (such as when using SQL Server Authentication), then you need to specify the appropriate name and password in the **Login name** and **Password** fields. Otherwise, leave these fields blank.

To refresh the **Data Source Name** list, click the **Refresh** button.

## Test Connection

Having specified the connection parameters, you could verify them to make sure they are correct. Click the **Test Connection** button to begin.

Please note that it only checks connectivity to the database server. In case of problems with access to the database while successfully connected to the database server, you won't see those problems in the **Test Connection** dialog box.



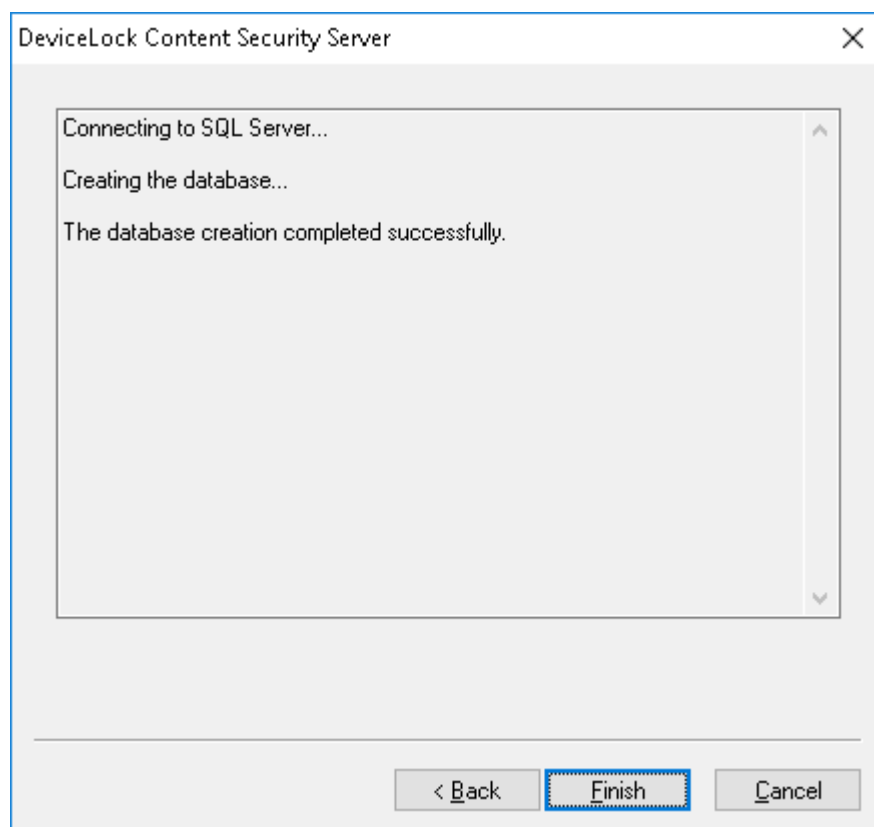
If some connection parameters were specified incorrectly, you may see one of these errors:

- **SQL Server does not exist or access denied** - An incorrect SQL Server name is specified in the **SQL Server name** parameter or the remote SQL Server's computer is not accessible. It is possible that you've specified the name of the computer running SQL Server but this SQL Server also has an instance name which should be specified as well (e.g. computer\instance).
- **Login failed for user 'COMPUTER\_NAME\$'** - Windows Authentication is selected but the user account used to run the DeviceLock Content Security Server service can't get access to the computer with SQL Server. It may happen when the service starts either under the SYSTEM user or on behalf of a user that doesn't have local administrative privileges on the remote SQL Server's computer.
- **Login failed for user 'user\_name'** - SQL Server Authentication is selected with either an incorrect SQL user name (login) or wrong password specified. Please note that SQL users are different from Windows users and you can't use the regular Windows account in the **Login name** parameter. SQL users exist only in SQL Server and to manage them you should use SQL Server management consoles (such as Microsoft SQL Server Management Studio).
- **Login failed for user 'user\_name'. The user is not associated with a trusted SQL Server connection** - SQL Server Authentication is but your SQL Server doesn't support this mode. You should either use Windows Authentication or allow your SQL Server to work in the mixed mode (SQL Server and Windows Authentication mode).
- **Login failed for user ''**. **The user is not associated with a trusted SQL Server connection** - The data source specified in **Data Source Name** is configured to use the SQL Server Authentication mode but the **Login name** parameter is empty.
- **Data source name not found and no default driver specified** - You've selected **System Data Source** from the **Connection type** list and specified either an empty or non-existent name in **Data Source Name**.

Click the **Next** button to apply changes and proceed to the last page.

## Completing configuration

It takes some time to create the database specified in **Database name** if it does not exist on this database server yet. If the database already exists and it has the proper format (i.e. was created by DeviceLock) then DeviceLock Content Security Server keeps all existing data and uses this database. If necessary, DeviceLock automatically updates the database to the latest version.



On this page of the configuration wizard you can observe the applying of the database settings specified, and view errors that might occur when configuring the database.

If some parameters on the previous page of the wizard were specified incorrectly, you might encounter the following errors:

- **CREATE DATABASE permission denied in database 'name'** - The user account (login) used to connect to SQL Server doesn't have sufficient rights to create the database. The login should have at least the dbcreator Server role (see **Server Roles** in **Login Properties** of Microsoft SQL Server Management Studio).
- **The server principal "user\_name" is not able to access the database "name" under the current security context** - The user account (login) used to connect to SQL Server doesn't have access to the existing database. The login should be mapped to this database (see **User Mapping** in **Login Properties** of Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** - The user account (login) used to connect to SQL Server doesn't have read/write access to the existing

database. The login should have at least db\_datareader and db\_datawriter Database roles (see **User Mapping in Login Properties** of Microsoft SQL Server Management Studio).

- **Invalid object name 'name'** - The database specified in the **Database name** parameter already exists on this SQL Server but has an incorrect format. It happens when you are trying to use the database that was not created by DeviceLock Content Security Server or if the database was corrupted.
- **DeviceLock Database has an unsupported format** - The database specified in the **Database name** parameter already exists but is outdated. This existing database has an unsupported format so it can't be automatically upgraded to the new format. You should either use another database or create a new one.
- **DeviceLock Database has a format that is not supported by the current server version** - The database specified in the **Database name** parameter already exists but it was created by the more recent version of DeviceLock Content Security Server. You should either use the latest version of DeviceLock Content Security Server or use another database (or create a new one).

Also, the wizard might display some of the SQL Server connection errors listed in the [Test Connection](#) section earlier in this document.

Use the **Back** button to return to the previous page of the wizard and make necessary changes.

If there are no errors, click the **Finish** button to close the wizard and continue the installation process.

Next, on the **Installation Wizard Completed** page, click **Finish** to complete the installation. On this page, you will have the option to go to the DeviceLock home page. This option is selected by default.

---

#### Note

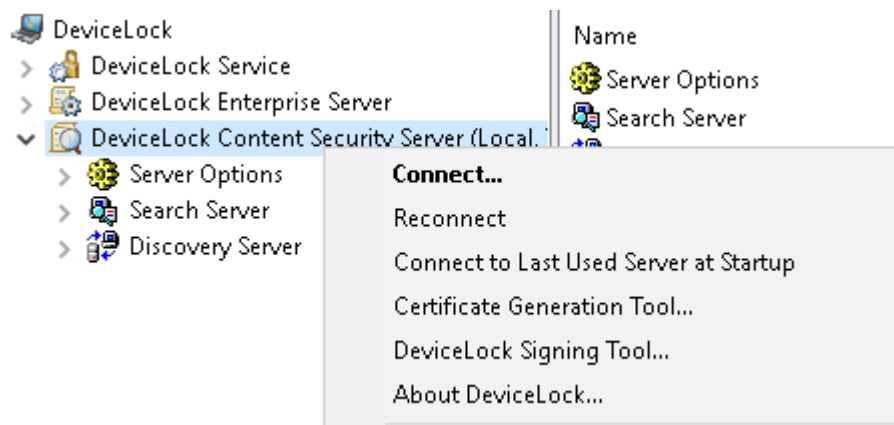
You can uninstall DeviceLock Content Security Server as follows:

- Use **Programs and Features** in Control Panel (**Add or Remove Programs** on earlier versions of Windows) to remove **DeviceLock Content Security Server**,  
- OR -
  - Select **Remove DeviceLock Content Security Server** on the Windows **Start** menu.
-

# Setting Up Discovery Server

## Navigating Discovery Server

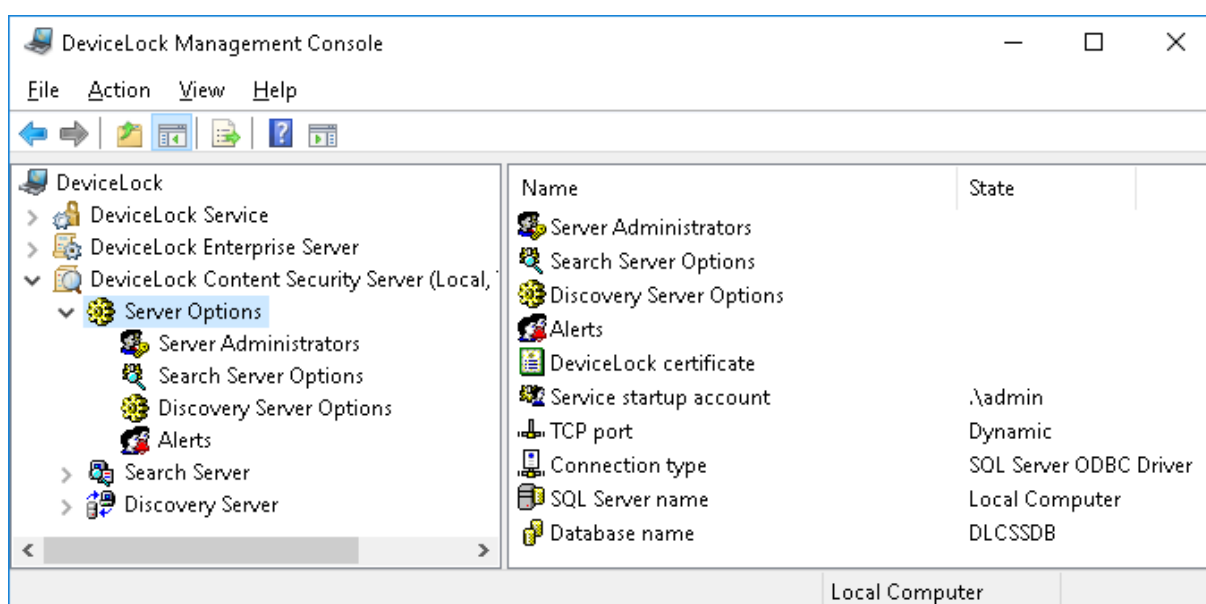
Before addressing the functionality of DeviceLock Discovery Server, you need to examine how to perform basic navigation. Use the **DeviceLock Content Security Server** node in DeviceLock Management Console to configure and use DeviceLock Content Security Server.



Right-click the **DeviceLock Content Security Server** node to display the following commands:

- **Connect** - Connects to the computer running DeviceLock Discovery Server.  
For detailed description of this command, refer to the [Connecting to Computers](#) section.  
When you connect to a computer where an old version of DeviceLock Discovery Server is installed, you may receive the following message: "The product version on the client and server machines does not match." In this case, you need to install the new version of DeviceLock Discovery Server on this computer. For installation instructions, refer to the [Installing DeviceLock Discovery](#) section.
- **Reconnect** - Connects to the currently connected computer once again.
- **Connect to Last Used Server at Startup** - Check this command to instruct DeviceLock Management Console to automatically connect to the last used server each time the console starts up.
- **Certificate Generation Tool** - Starts a tool for generating DeviceLock Certificates. For details, refer to the [Generating DeviceLock Certificates](#) section.
- **DeviceLock Signing Tool** - Starts a tool to grant users temporary access to devices and to sign files containing DeviceLock Service settings. For details, refer to the [DeviceLock Signing Tool](#) section.
- **About DeviceLock** - Displays the dialog box with information about the DeviceLock version and your licenses.

Expand the **DeviceLock Content Security Server** node, and select the **Server Options** node:



You can use this node to configure the following common settings for DeviceLock Search Server and Discovery Server:

- **Server Administrators** - Use this setting to specify the server administrators and their associated access rights.
- **Search Server Options** - Use this option to configure settings related to full-text search.
- **Discovery Server Options** - Use this option to configure settings related to content discovery.
- **Alerts** - Use this option to configure delivery settings for alerts.
- **DeviceLock certificate** - Use this setting to install, change or remove the DeviceLock Certificate pair.
- **Service startup account** - Use this setting to specify the startup account information, such as the account name and the password, for the server service.
- **TCP port** - Use this setting to specify the TCP port that the DeviceLock Management Console uses to connect to the server.
- **Connection type** - Use this setting to choose the ODBC driver or system data source to connect to the DeviceLock Content Security Server's database.
- **SQL Server name** - Use this setting to specify the DeviceLock Content Security Server's database server. This setting is available for the ODBC driver connection type.
- **System Data Source** - Use this setting to specify the data source to access the DeviceLock Content Security Server's database server. This setting is available for the system data source connection type.
- **Database name** - Use this setting to specify the name of the DeviceLock Content Security Server's database.
- **SQL Server login** - Use this setting to specify the login and password to access the DeviceLock Content Security Server's database. This setting is available for the SQL Server Authentication mode.



Expand the **Server Options** node and select the **Discovery Server Options** node. You can use this node to configure the following settings specific to DeviceLock Discovery Server:

- **DeviceLock Enterprise Server(s)** - Use this setting to specify one or more DeviceLock Enterprise Servers that host the fingerprints database.
- **Discovery Server license(s)** - Use this setting to install the required number of DeviceLock Discovery licenses.
- **Log options** - Use this setting to specify event logging options for Discovery Server. Enables you to configure the types of events to be logged.
- **E-Mail Message for Alerts** - Use this setting to configure the template of e-mail messages used to alert administrators about discovered content.
- **Syslog Message for Alerts** - Use this setting to configure the syslog message template of alerts.
- **Discovery notification message** - Use this setting to configure the template of a tray notification message shown to the currently logged in users when a discovery event occurs.
- **Data collection interval** - Use this setting to specify the interval of collecting data from discovery agents.
- **Binary files content inspection** - Use this setting to enable keywords- and pattern-based content discovery for text held in arbitrary binary files.

## General Settings

There are three types of configuration settings for the DeviceLock Content Security Server:

- **General settings** - Affect the operation of the DeviceLock Content Security Server as a whole. The current section provides instructions for managing these settings.
- **Search Server settings** - Affect the operation of the Search Server, a part of the DeviceLock Content Security Server. For details, see [Managing Search Server Settings](#).
- **Discovery Server settings** - Affect the operation of the Discovery Server. For instructions on how to manage these settings, see [Discovery Server Options](#).

The administrator can configure general server settings when installing the DeviceLock Content Security Server, or use the DeviceLock Management Console to configure and/or modify them after the server has been installed and is functioning.

---

### Note

- Only server administrators with sufficient rights can manage and use the DeviceLock Content Security Server.
  - To begin, connect the DeviceLock Management Console to the computer running the DeviceLock Content Security Server: Right-click **DeviceLock Content Security Server**, and then click **Connect**. For more information, see [Connecting to Computers](#).
- 

With the DeviceLock Management Console, the administrator can perform the following server configuration tasks:

- Configure which users have access to the DeviceLock Content Security Server.
- Change the startup account information, such as the account name or the password, for the DeviceLock Content Security Server service.
- Install or remove the DeviceLock certificate to authenticate communications between the DeviceLock Content Security Server and the DeviceLock Enterprise Server.
- Change the TCP port to connect the DeviceLock Management Console to the DeviceLock Content Security Server.
- View or change the DeviceLock Content Security Server's database connection settings.

One can perform these tasks individually or collectively.

To perform the tasks collectively, use the DeviceLock Content Security Server configuration wizard. This is the wizard that starts automatically when installing or upgrading the DeviceLock Content Security Server.

### ***To perform configuration tasks collectively***

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, right-click **Server Options**, and then click **Properties**.  
*The first page of the wizard appears.*
3. Move through the wizard pages. After completing each page, move to the following one by clicking **Next**, or move to the preceding one by clicking **Back**. On the final page, click **Finish** to complete the wizard.  
For description of the wizard pages, see the [Perform Configuration and Complete Installation](#) section in the DeviceLock Content Security Server installation instruction.

Using the DeviceLock Management Console, the administrator can perform the following tasks to configure individual server settings:

- [Configuring access to the DeviceLock Content Security Server](#)
- [Setting the service startup account](#)
- [Installing or removing a DeviceLock certificate](#)
- [Configuring the TCP Port setting](#)
- [Managing the database connection settings](#)

## Configuring access to the DeviceLock Content Security Server

The administrator can specify the users who are allowed to access the DeviceLock Content Security Server. This restricts outsiders from accessing or damaging the server.

### ***To configure which users have access to the server***

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, do one of the following:
  - Select **Server Options**. In the details pane, double-click **Server Administrators** or right-click **Server Administrators** and then click **Properties**.

- OR -

- Expand **Server Options**. Under **Server Options**, right-click **Server Administrators** and then click **Properties**.

3. In the **DeviceLock Content Security Server** dialog box that appears, do the following:

**To enable default security**

- Select the **Enable Default Security** check box.

If default security is enabled, members of the local Administrators group will have full access to DeviceLock Content Security Server.

**To restrict access to the server to specific users**

- a. Clear the **Enable Default Security** check box.
- b. Under **Users**, click **Add** to add the specific users to be allowed access to the DeviceLock Content Security Server.
- c. In the **Select Users or Groups** dialog box that appears, in the **Enter the object names to select** box, type the name of the user or group, and then click **OK**.  
The selected users/groups become server administrators, which are listed under **Users** in the **DeviceLock Content Security Server** dialog box. Server administrators are authorized to perform the tasks related to configuring and using the DeviceLock Content Security Server and, by default, they have full access to the server.

To change the server access level for a particular administrator, select the respective user or group under **Users**, and then choose from the following options in the list of access rights:

- **Full access** - Allows the user or group to install and uninstall the DeviceLock Content Security Server, connect to it by using the DeviceLock Management Console, and perform any actions on the server, such as: view and change server settings; create and run search queries and tasks; view and change content detection settings; create and run discovery tasks and reports.
- **Change** - Same as full access to the server with the exception of the right to make changes to the list of server administrators or change the level of access to the server for the users or groups already in that list.
- **Read-only** - Allows the user or group to connect to the DeviceLock Content Security Server by using the DeviceLock Management Console; view server settings; run search queries; view and run existing search tasks; view content detection settings; view discovery reports and manually create new reports based on the existing reports and data already prepared by discovery tasks. This option does not give the right to run discovery tasks, make any changes on the server, or create a new index for the Search Server.

For users and groups with **Change** or **Read-only** access, the **Shadow Data Access** option can be selected to allow access to shadow copies and user activity records. The users and groups with this option selected are allowed to search the content of shadow copies and user activity records, and open, view, and save shadow copies and user activity records from search results. Without access to shadow data, DeviceLock Content Security Server administrators cannot open, view, or save shadow copies and records of user activity. Search results do not have the **Open**, **Save**, and **View** links, and asterisks are displayed instead of text snippets of shadow copies and user activity records. Logins and passwords in document parameters for user activity records are also replaced with asterisks.

---

**Note**

We strongly recommend that administrators of DeviceLock Content Security Server be given local administrator rights.

---

To revoke server administrator rights from a particular user or group, select that user or group in the **Users** area, and then click the **Delete** button.

One can select multiple users or groups by holding down the SHIFT key or the CTRL key while clicking them.

4. Click **OK**.

## Setting the service startup account

Over time, the administrator might need to change the account that was specified as the service startup account when installing the DeviceLock Content Security Server. It is also possible to change the password of the service startup account.

### *To change the service startup account or password*

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options**.
3. In the details pane, double-click **Service startup account** or right-click **Service startup account** and then click **Properties**.
4. In the **DeviceLock Content Security Server** dialog box that appears, do the following:

#### **To change the service startup account**

- a. In the **Log on as** area, click **Browse**.
- b. In the **Select User** dialog box that appears, in the **Enter the object name to select** box, type the name of the user, and then click **OK**.

The selected user is displayed in the **This account** box in the **DeviceLock Content Security Server** dialog box.

We recommend the use of an account with administrator rights on all computers running the DeviceLock Enterprise Server. In an Active Directory environment, we recommend the use an account that is a member of the Domain Admins group. Otherwise, DeviceLock certificate authentication should be used.

#### **To change the service account password**

- a. In the **Log on as** area, type a new password in the **Password** box.
- c. Re-type the new password in the **Confirm password** box.

#### **To assign the Local System account to the server service**

- In the **Log on as** area, click **Local System account**.

---

**Note**

If the service uses the Local System account, the Discovery Server:


- Cannot access Discovery Agents running on remote computers and must use the DeviceLock Certificate for authentication on it.
  - Cannot install or remove Discovery Agents on remote computers.
- 

5. Click **OK**.

## Installing or removing a DeviceLock certificate

The Discovery Server may not be able to access the Discovery Agent due to insufficient access rights of the service startup account of the DeviceLock Content Security Server. In this case, DeviceLock certificate authentication should be set up by installing the private key of a DeviceLock certificate on the DeviceLock Content Security Server. The public key of that certificate must be installed for the DeviceLock Service on each computer to be scanned by the Discovery Agent. For details on DeviceLock certificates, see [DeviceLock Certificates DLP](#).

### *To install or remove DeviceLock Certificate on DeviceLock Content Security Server*

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options**.
3. In the details pane, double-click **DeviceLock certificate** or right-click **DeviceLock certificate** and then click **Properties**.
4. In the **DeviceLock Content Security Server** dialog box that appears, do the following:
  - To install the private key of the DeviceLock certificate**
    - a. Next to the **Certificate Name** box, click the  button to open the **Select the DeviceLock Certificate file** dialog box and browse for the file to use.
    - b. In the **Select the DeviceLock Certificate file** dialog box, locate and select the certificate file, and then click **Open**.
  - To remove the private key of the DeviceLock certificate**
    - Next to the **Certificate Name** box, click **Remove**.
5. Click **OK**.

## Configuring the TCP Port setting

Over time, the administrator might need to change the TCP port that the DeviceLock Management Console uses to connect the DeviceLock Content Security Server.

### *To change the TCP port for connecting the console*

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options**.
3. In the details pane, double-click **TCP port** or right-click **TCP port** and then click **Properties**.

4. In the **Connection Settings** area of the **DeviceLock Content Security Server** dialog box that appears, do one of the following:
  - Click **Dynamic ports** to use a dynamic port selection.
  - OR -
  - Click **Fixed TCP port** to use a specified port. Then, type the desired port number in the **Fixed TCP port** box.By default, the DeviceLock Content Security Server uses TCP port 9134.
5. Click **OK**.

## Managing the database connection settings

A database connection is required for the Discovery Server to function. If there is no connection to the database, the Discovery Server is unavailable. The administrator can use the console to view or change the database connection settings.

### *To view or change the database connection settings*

1. In the console tree, expand **DeviceLock Content Security Server**.
2. Under **DeviceLock Content Security Server**, select **Server Options**.
3. In the details pane, double-click any of these options: **Connection type**, **SQL Server name**, **Database name**, or **SQL Server login**. Alternatively, right-click an option, and then click **Properties**.
4. In the dialog box that appears, view or change the following connection settings:
  - **Database name** - The name of the DeviceLock Content Security Server's database.
  - **Connection type** - Determines whether to use an ODBC driver or system data source to connect to the DeviceLock Content Security Server's database server. Further options depend upon the selected connection type.
  - **SQL Server name** - The name of the database server (if using an ODBC driver). Empty name indicates a database server running on the same computer as the DeviceLock Content Security Server.
  - **Windows authentication / SQL Server authentication** - The authentication mode to use on SQL Server (for Microsoft SQL Server ODBC driver).
  - **Data source name** - The name of the system data source (if using a system data source).
  - **Login name, Password** - Login and password to access the database (if using the SQL Server Authentication mode).
  - Click **Next**, wait while the console completes the connection, and then click **Finish**.

For details on the database connection settings, see the [Database settings](#) section in the DeviceLock Content Security Server installation instruction.

## Discovery Server Options

The following Discovery Server options are available:

- **DeviceLock Enterprise Server(s)** - Allows you to specify one or more DeviceLock Enterprise Servers that host the fingerprints database.
- **Discovery Server license(s)** - Allows you to install your license for DeviceLock Discovery.
- **Log options** - Allows you to specify the types of event to record to the Discovery tasks log.
- **E-Mail Message for Alerts** - Allows you to customize the e-mail message template for Discovery alerts.
- **Syslog Message for Alerts** - Allows you to customize the syslog message template for Discovery alerts.
- **Discovery notification message** - Allows you to customize the Discovery message that pops up in the system notification area of the computer being scanned.
- **Data collection interval** - Allows you to specify the time interval through which Discovery Agent begins to report the availability of new data for transmission to the Discovery server.
- **Binary Files Content Inspection** - Allows you to enable keywords- and pattern-based content discovery for text held in arbitrary binary files.

To start configuring an option, double-click that option, or right-click it and use commands on the shortcut menu that appears.

Managing Discovery Server options involves the following tasks:

- [Specifying Digital Fingerprints Database Server\(s\)](#)
- [Installing DeviceLock Discovery licenses](#)
- [Configuring log options](#)
- [Setting up alert and notification messages](#)
- [Setting the data collection interval](#)
- [Enabling binary files content inspection](#)

## Specifying Digital Fingerprints Database Server(s)

To use digital fingerprints for content discovery, DeviceLock Discovery requires at least one DeviceLock Enterprise Server to be specified that hosts the fingerprints database. For details on the digital fingerprinting technique, refer to the [Digital Fingerprints](#) section.

To specify servers that host the fingerprints database, right-click **DeviceLock Enterprise Server(s)** in **Discovery Server Options** and then click **Properties**, or double-click **DeviceLock Enterprise Server(s)**. Then, use the dialog box that appears to view or change the list of servers.

To add a server to the list, type the name of the computer on which the DeviceLock Enterprise Server is installed. You could type, for instance, the computer's fully qualified domain name (FQDN), short name or IP address. To add multiple servers, type computer names separated by a semicolon (;).

Individual computer names can be changed or removed from the list. To clear the list, click the **Remove** button.

## Installing DeviceLock Discovery licenses

To use content scanning and discovery, you need to purchase special DeviceLock Discovery licenses, corresponding to the number of computers or network resources to be scanned (hereinafter, only computers are mentioned).

DeviceLock Discovery licensing is based on the number of computers that DeviceLock Discovery will scan. One license allows you to scan one computer, regardless of whether the entire computer is scanned or a specific folder on that computer.

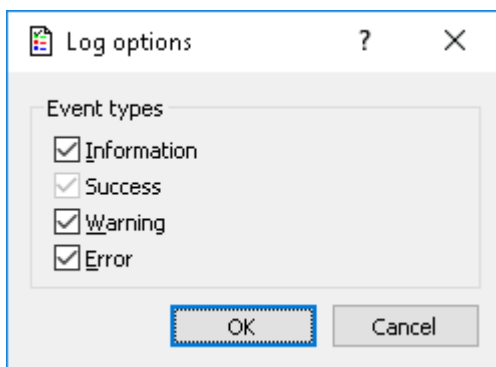
Depending on the total number of computers that should be scanned by DeviceLock Discovery, you must purchase the appropriate number of licenses. If multiple DeviceLock Discovery licenses are used, the number of computers to be scanned will be summed based on the number of licenses. The trial period for DeviceLock Discovery is 30 days. During the trial period, you can scan up to two computers. You can purchase and install additional DeviceLock Discovery licenses at any time.

You can install additional DeviceLock Discovery licenses by opening the **Discovery Server Options** node and then double-clicking the **Discovery Server license(s)** parameter. In the dialog box that appears, click the **Load License(s)** button to select the license file. It is possible to load several license files in series - one by one.

After you have loaded your license files, the dialog box displays the license information summary where **Total license(s)** is the total number of installed licenses while **Used license(s)** is the number of licenses currently in use for scanning computers or network devices with DeviceLock Discovery.

## Configuring log options

Double-click the **Log options** parameter to open the dialog box where you can specify the types of event to record to the Discovery tasks log.



To enable or disable the recording of particular event types, select or clear respective check boxes:

- **Information** - Certain action performed.
- **Success** - Task or operation completed successfully.
- **Warning** - A problem might occur unless action is taken.
- **Error** - A problem has occurred.



---

**Note**

The events indicating success are always recorded, therefore the Success check box is selected and cannot be cleared.

---

## Setting up alert and notification messages

Network administrators as well as users on computers being scanned can be notified about certain events. Two kinds of notification are available:

- **Alerts** are SNMP traps, syslog messages or email messages that the DeviceLock Discovery Agent generates to help administrators keep track of the scanning process and be notified immediately if certain types of content are discovered.
- **Notifications** are system messages displayed to the current users on the computers being scanned, in a pop-up window next to the system clock in the taskbar. Notifications appear when the DeviceLock Discovery Agent detects content matches with discovery rules that are in effect.

---

**Note**

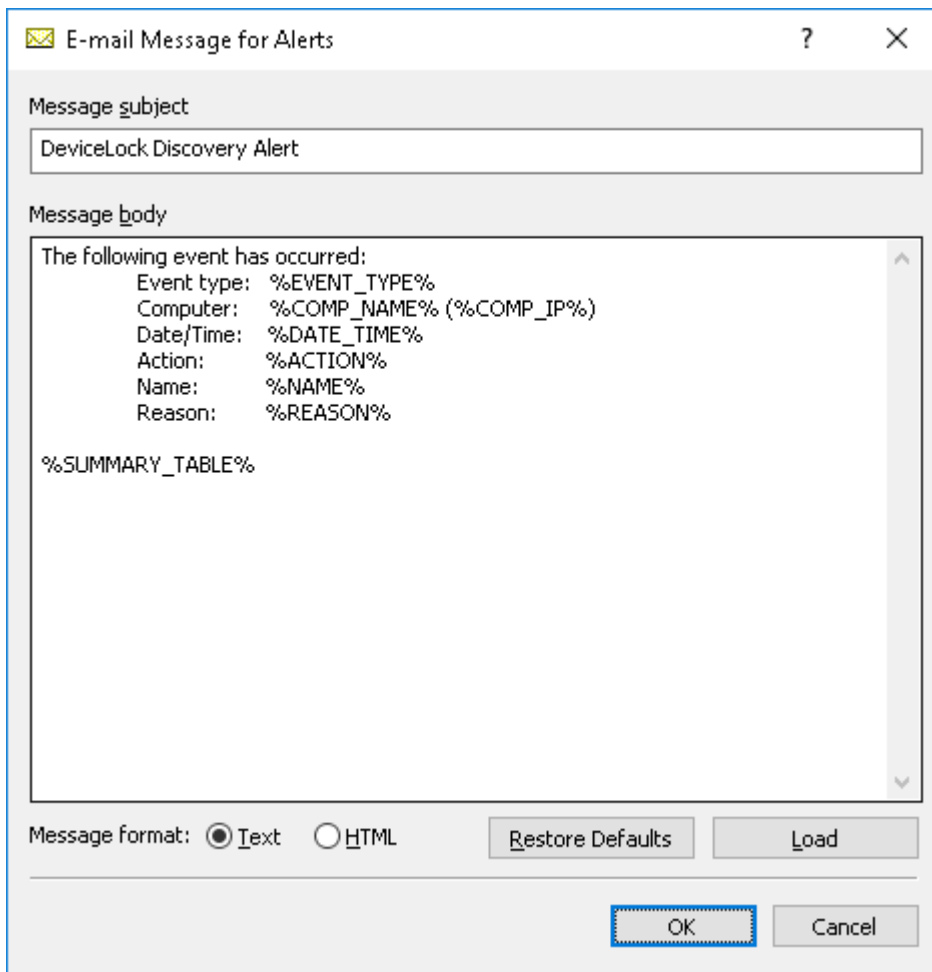
DeviceLock displays user notifications when scanning with the Discovery Agent only. In the case of agentless scanning, user notifications are not displayed.

---

In **Discovery Server Options**, the contents of alert and notification messages can be configured by using the respective options.

### ***To configure email message for alerts***

1. Double-click the **E-Mail Message for Alerts** item in the **Discovery Server Options** node.  
- OR -  
Right-click the **E-mail Message for Alerts** item in the **Discovery Server Options** node, and select **Properties** from the shortcut menu.  
*The E-mail Message for Alerts dialog box appears.*



2. In the **E-mail Message for Alerts** dialog box, edit the template of the e-mail message, and click **OK**.

The template contains the following information:

- **Message subject** - The text used in the **Subject** line of the e-mail message. The default message subject is "DeviceLock Discovery Alert".
- **Message body** - The text used in the body of the e-mail message. DeviceLock can send either the plain text body or an HTML version of the message body. The message body includes a static text and macros. The default static text in the message body is "The following event has occurred".

You can use the following predefined macros in the **Subject** line and/or the body of the e-mail message:

- **%EVENT\_TYPE%** - The class of event: either **Success** if the action was successfully applied to the discovered content, or **Failure** if the action could not be applied.
- **%COMP\_NAME%** - The name of the computer on which the file was discovered.
- **%COMP\_FQDN%** - The fully-qualified domain name of the computer on which the file was discovered.
- **%COMP\_IP%** - A comma-separated list of all network addresses (IPs) associated with the computer.

- **%DATE\_TIME%** - The date and time that the discovery event occurred. The date and time are displayed based on the client computer's regional and language settings.
- **%ACTION%** - The action applied to the identified file.
- **%NAME%** - The name of the file to which the action was applied.
- **%REASON%** - The cause of the event (the name of the rule that was triggered by the file).
- **%SUMMARY\_TABLE%** - A table detailing and visualizing individual events for consolidated alerts.

These macros are replaced with their actual values at the message generation time.

3. Select the **Text** or **HTML** email format by using the **Message format** option.
4. If needed, restore the default template by clicking **Restore Defaults**, or load a template from a file by clicking the **Load** button.

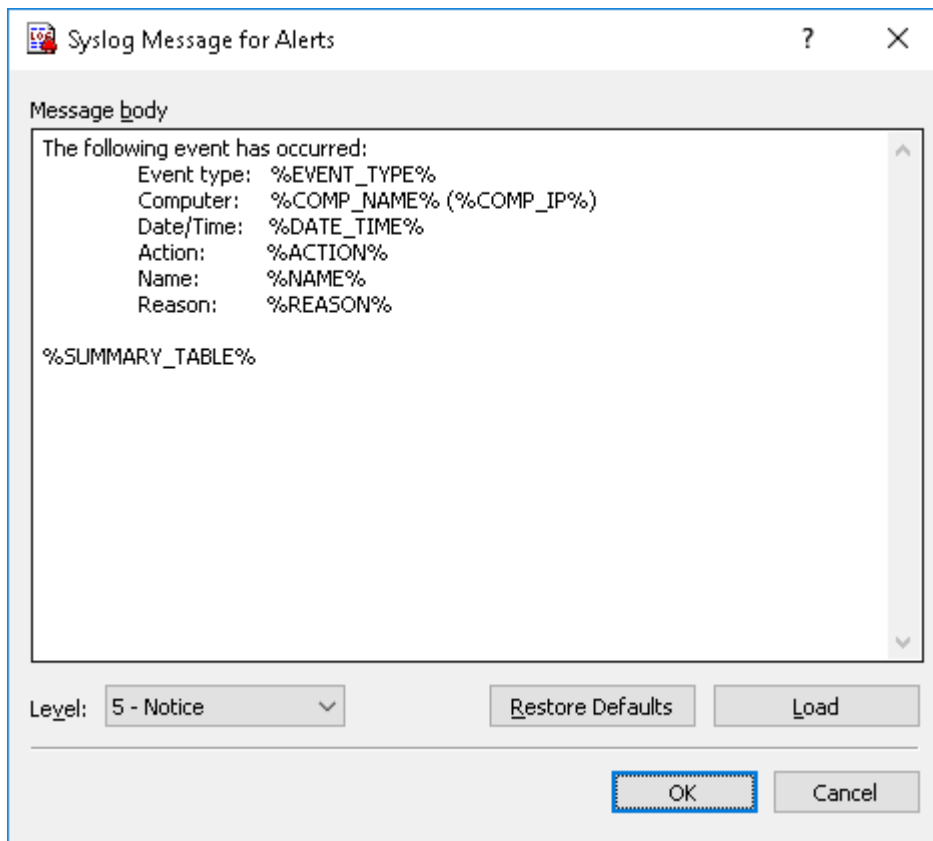
A template can be loaded from a tab-delimited text file containing plain text or HTML.

### ***To configure syslog message for alerts***

1. Double-click on the **Syslog Message for Alerts** item in the **Discovery Server Options** node.  
- OR -

Right-click the **Syslog Message for Alerts** item in the **Discovery Server Options** node, and select **Properties** from the shortcut menu.

*The Syslog Message for Alerts dialog box appears.*



2. In the **Syslog Message for Alerts** dialog box, edit the template of the message, and click **OK**.  
The template contains the following information:

- **Message body** - The text used in the body of the message. The message body includes a static text and macros. The default static text in the message body is "The following event has

occurred”.

You can use the following predefined macros in the body of the syslog message:

- %EVENT\_TYPE% - The class of event: either **Success** if the action was successfully applied to the discovered content, or **Failure** if the action could not be applied.
- %COMP\_NAME% - The name of the computer on which the file was discovered.
- %COMP\_FQDN% - The fully-qualified domain name of the computer on which the file was discovered.
- %COMP\_IP% - A comma-separated list of all network addresses (IPs) associated with the computer.
- %DATE\_TIME% - The date and time when the discovery event occurred. The date and time are displayed based on the client computer’s regional and language settings.
- %ACTION% - The action applied to the identified file.
- %NAME% - The name of the file to which the action was applied.
- %REASON% - The cause of the event (the name of the rule that was triggered by the file).
- %SUMMARY\_TABLE% - A table detailing and visualizing individual events for consolidated alerts.

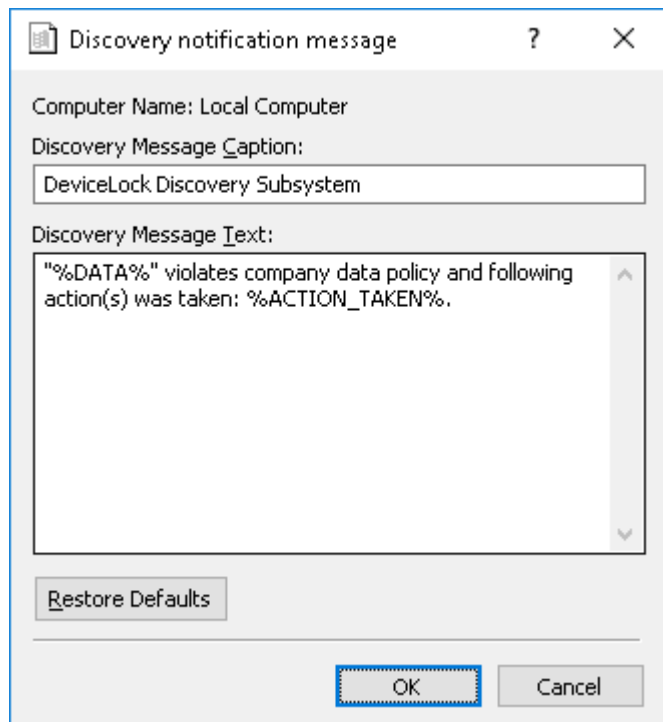
These macros are replaced with their actual values at the message generation time.

3. Select the message severity level using **Level** drop-down menu.
4. If needed, restore the default template by clicking **Restore Defaults**, or load a template from a file by clicking the **Load** button.

A template can be loaded from a tab-delimited text file containing plain text.

### ***To configure the discovery notification message***

1. Double-click the **Discovery notification message** item in the **Discovery Server Options** node.  
*The Discovery notification message dialog box appears.*



2. In the **Discovery notification message** dialog box, specify the **Caption** and **Text** of the notification message. This message pops up in the system notification area of a computer being scanned, and is visible to all users who are currently logged on to that computer. Along with static text, you can use the following predefined macros in the text of the notification message:
  - %DATA% - The name of the file that triggered the message.
  - %ACTION\_TAKEN% - The name of the action(s) applied to that file.

---

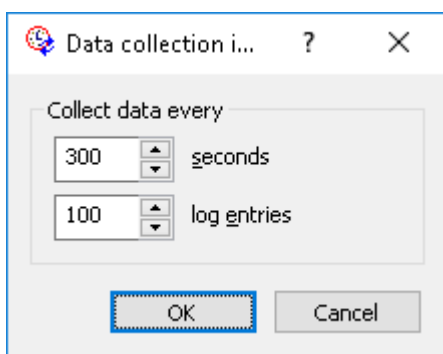
**Note**

Notification messages are not displayed in case of agentless scanning. In case of scanning a terminal server, notification messages are displayed to all users connected to the terminal server.

---

## Setting the data collection interval

You can configure the interval of discovery agents notifying the Discovery Server about new data. To change data collection settings, double-click the **Data collection interval** item in the **Discovery Server Options** node. The **Data collection interval** dialog box will appear.



Under **Collect data every**, specify the time in seconds that should pass after a discovery task is started and before the scanning agents will start notifying the Discovery Server about new data. The default value is 300 seconds.

You can also specify the number of log entries to be accumulated before Discovery Agents will notify Discovery Server. Discovery Agent logs certain events during its work. Discovery Server users may specify additional logging rules, e.g. instructing the product to add a log entry if certain types of content are encountered. This setting configures the number of accumulated log entries that would cause Discovery Agents to notify the Discovery Server, after which the Discovery Server would collect information from the notifying Agent. The default value is 100 log entries.

The time in seconds and the number of log entries parameters are used concurrently. The data will be sent as soon as any one of the two conditions is met.

## Enabling binary files content inspection

The **Binary Files Content Inspection** option allows for inspecting text content held in arbitrary binary files. When this option is disabled, DeviceLock performs keywords- and pattern-based content discovery for only Unicode text held in known file types. For a list of known file types, see

Expansive coverage of multiple file formats and data types in the [ContentLock and NetworkLock](#) section.

When this option is enabled, DeviceLock performs keywords- and text pattern-based content discovery for text held in any binary files, regardless of text encoding (Unicode or non-Unicode). In this case, content discovery may take considerably longer to complete.

---

**Note**

This option affects discovery rules that employ keywords groups, pattern groups and/or complex content groups containing those group types. For details regarding discovery rules, see [Rules and Actions](#).

---

To enable or disable this option, double-click the **Binary Files Content Inspection** item in the **Discovery Server Options** list, or right-click that item and then choose **Enable** or **Disable**.

## Alerts

The following alert options are available:

- **SNMP** - Allows you to configure SNMP transport for alerts.
- **SMTP** - Allows you to configure delivery of alerts via e-mail using an SMTP server.
- **Syslog** - Allows you to configure the forwarding of alerts to a syslog server.
- **Delivery retry parameters** - Allows you to configure server actions in case of alert delivery failure.

To start configuring an option, double-click that option, or right-click it and use commands on the shortcut menu that appears.

## General Information

When scanning computers, DeviceLock Discovery can notify network administrators of certain events by issuing alerts. You can define alerts to automatically notify you if a scanning agent discovers content matching one of the defined discovery rules. Real-time alerting simplifies network administration and helps you respond faster and more efficiently to security incidents and policy violations.

Discovery Agents can send alerts notifying administrators of content discovery. Alerts can be sent to their intended recipients through e-mail or SNMP traps. Also, alerts can be sent to a syslog server.

To enable DeviceLock Content Security Server to send alert notifications, you should do the following:

- Decide how to be notified when alert conditions occur: through SNMP traps, e-mail or syslog.
- To be notified through SNMP traps, configure DeviceLock Content Security Server for SNMP support and specify the SNMP server to send traps to. For details, see [Alerts Settings: SNMP](#).

---

**Note**

This manual assumes a basic understanding of the Simple Network Management Protocol (SNMP) and related network management concepts.

---

- To be notified through e-mail, configure e-mail notifications by specifying SMTP Server and e-mail notification settings and defining the e-mail templates. For details, see [Alerts Settings: SMTP](#).
  - To be notified through syslog, configure DeviceLock Content Security Server for syslog and specify the syslog server to send alerts to. For details, see [Alerts Settings: Syslog](#).
- 

**Note**

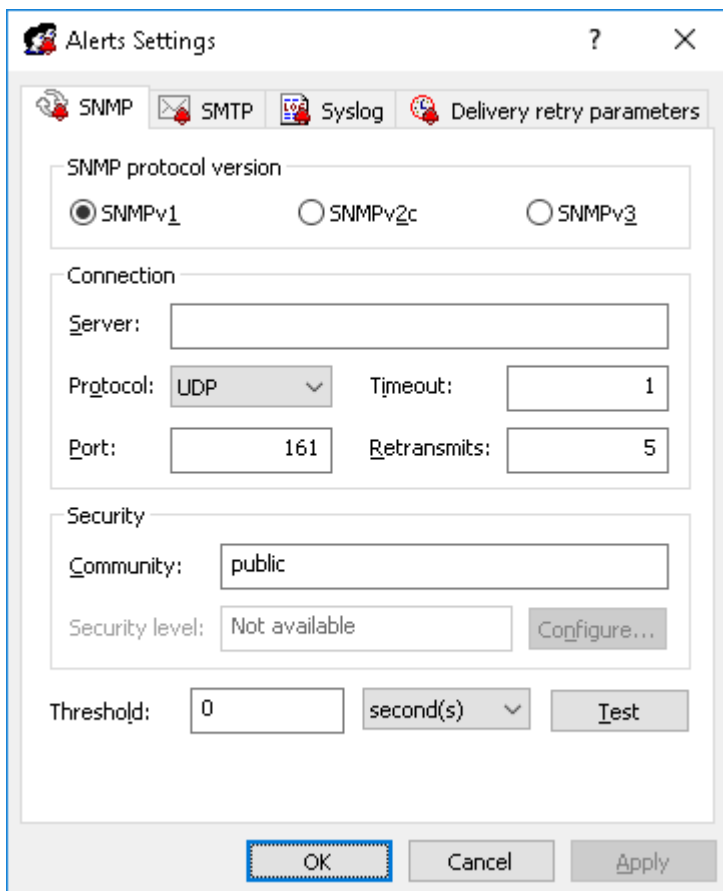
This manual assumes a basic understanding of syslog and related message logging concepts.

---

- Configure server actions in case of alert delivery failure, such as the delivery retry count, delivery retry interval, and the amount of time an undelivered notification is kept in the queue for delivery. For details, see [Alerts Settings: Delivery retry parameters](#).

## Alerts Settings: SNMP

Use the **SNMP** tab in the **Alerts Settings** dialog box to configure DeviceLock Content Security Server for SNMP support.




The image shows the 'Alerts Settings' dialog box with the 'SNMP' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are four tabs: 'SNMP' (selected), 'SMTP', 'Syslog', and 'Delivery retry parameters'. The 'SNMP' tab contains the following settings:

- SNMP protocol version:** Three radio buttons are present: 'SNMPv1' (selected), 'SNMPv2c', and 'SNMPv3'.
- Connection:** A section containing:
  - Server:** An empty text input field.
  - Protocol:** A dropdown menu currently showing 'UDP'.
  - Timeout:** A text input field containing the value '1'.
  - Port:** A text input field containing the value '161'.
  - Retransmits:** A text input field containing the value '5'.
- Security:** A section containing:
  - Community:** A text input field containing the value 'public'.
  - Security level:** A dropdown menu showing 'Not available', with a 'Configure...' button to its right.
- Threshold:** A text input field containing '0', followed by a dropdown menu showing 'second(s)', and a 'Test' button.

At the bottom of the dialog are three buttons: 'OK' (highlighted with a red box), 'Cancel', and 'Apply'.

To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.
- Select **Alerts** in the console tree, and then click **Manage**  on the toolbar.
- Select **Alerts** in the console tree; then, in the details pane, right-click **SNMP** and click **Manage**.
- Select **Alerts** in the console tree, and then double-click **SNMP** in the details pane.

DeviceLock supports SNMPv1, SNMPv2c, and SNMPv3 protocols. You can configure DeviceLock Content Security Server to automatically send alert notifications to the specified SNMP server when alert conditions occur. These alerts are sent only when all of the following conditions are met:

- The SNMP server is set up to receive traps.
- The remote computer running the SNMP server is accessible from computers where the discovery task is being performed (by the Agent) or from the server (in case of agentless scanning).
- Alerts have been configured to be sent through SNMP traps.

Complete the **SNMP** tab as follows:

- **SNMP protocol version** - Choose the SNMP protocol version required by your SNMP server. Available options are: **SNMPv1**, **SNMPv2c**, and **SNMPv3**.
- **Connection** - Supply the SNMP server-related information:
  - **Server** - The SNMP sever to send traps to. In the **Server** box, type the SNMP server host name or IP address.
  - **Protocol** - The transport protocol for passing data between DeviceLock and the SNMP server. Available options are: **UDP** and **TCP**.
  - **Timeout** - The time (in seconds) that DeviceLock waits for the SNMP server to reply before retransmitting the data packet. The default value is 1 second.
  - **Port** - The port on which the SNMP server listens for traps. The default port is 161.
  - **Retransmits** - The number of times a request is re-sent to the SNMP server, if the server is not responding (applies only to the **TCP** protocol). The default value is 5.
- **Security** - Configure SNMP security settings:
  - **Community** (if SNMPv1 or SNMPv2c is selected) - The SNMP community name to use for authentication with the SNMP server. The default value is `public`.
  - **User name** (if SNMPv3 is selected) - The name of the user account to use for authentication with the SNMP server. To specify a user name, click the **Configure** button next to the **Security level** box. If authentication is not required, a user name may not be specified.
  - **Security level** (if SNMPv3 is selected) - A value indicating the security level of SNMP communication. Possible values:
    - **No security** - Communication using neither authentication nor encryption.
    - **Authentication** - Communication using authentication without encryption.
    - **Authentication and Privacy** - Communication using both authentication and encryption.
  - **Configure** (if SNMPv3 is selected) - Click the **Configure** button next to the **Security level** box, to specify the following settings:



- **Security user name** - Supply the name of the user account to use for authentication with the SNMP server. If authentication is not required, this field can be left blank.
  - **Context name** - Supply the context name, as required by SNMP server.
  - **Context engine ID** - Supply the context engine ID, as required by SNMP server.
  - **Authentication protocol** - Choose the protocol used to encrypt the authentication with the SNMP server. Available options:
    - **None** - Security level of **No security**.
    - **HMAC-SHA** - Security level of **Authentication** or **Authentication and Privacy**, depending upon the **Privacy protocol** setting.
  - **Password/ Confirm password** - Supply the password of the user account to use for authentication with the SNMP server (applies to the **Authentication protocol** setting).
  - **Privacy protocol** - Choose the protocol used to encrypt data for SNMP communication. Available options:
    - **None** - Security level of **No security** or **Authentication**, depending upon the **Authentication protocol** setting.
    - **CBC-AES-128** - Security level of **Authentication and Privacy**, requires the **Authentication protocol** setting other than **None**.
  - **Password/ Confirm password** - Supply the password for data encryption (applies to the **Privacy protocol** setting).
- **Threshold** - Specify the time interval (in hours, minutes or seconds) used for event consolidation when generating alerts. DeviceLock consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:
    - a. The events are of the same type, either **Success** for actions successfully performed on discovered content, or **Failure** for failed actions.
    - b. The **Reason** and **Computer** of the events being wrapped are the same.  
The default value is 0 seconds.
  - **Test** - Click to send a test SNMP trap to verify that DeviceLock is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:
    - The test can complete successfully, meaning that a test SNMP trap was successfully sent using the configured SNMP trap parameters. The resulting message states: "Test SNMP alert was successfully sent."
    - The test can fail, meaning that a test SNMP trap was not sent. The resulting message states: "Test SNMP alert was not sent due to error: <error\_description>."

SNMP traps by DeviceLock Discovery are presented in the Management Information Base (MIB) format. MIB for DeviceLock Discovery has the object identifier (OID) 1.3.6.1.4.1.60000 or iso.org.dod.internet.private.enterprise.DeviceLock, and it contains the following branch nodes:

- products(1)
- discoveryAgent(1)

- alerts(1) - This node contains one instance of each of the following MIB objects:
  - eventType(1) - The class of an event: either Success for allowed access or Failure for denied access. Note that the value of eventType is displayed as a numeric value rather than a text string: 8 indicates Success, 16 indicates Failure.
  - computerName(2) - The name of the computer from which the event was received.
  - action(3) - The user's activity type.
  - name(4) - The name of the discovered object.
  - reason(5) - The cause of the event.
  - datetime(6) - The date and time (in the RFC3339 date/time format) when the content discovery event has occurred.

---

### Note

These MIB objects correspond to the column data in the [Tasks Log Viewer](#).

---

A trap is sent just once each time an event associated with an alert occurs. Below is an example of the SNMP alert.

```


⚡ Specific: 1
    Message reception date: 21.02.2014
    Message reception time: 13:25:34.862
    ⌚ Time stamp: 274 days 06h:37m:07s.29th
    ⚡ Message type: Trap (v1)
    Protocol version: SNMPv1
    Transport: IP/UDP
    🖥 Agent
        Address: 10.10.30.16
        Port: 59467
    🖥 Manager
        Address: 192.168.209.1
        Port: 0
    🔑 Community: public
    🖥 SNMPv1 agent address: 10.10.30.16
    📁 Enterprise: enterprises.60000
    📁 Bindings (6)
        🟢 Binding #1: enterprises.60000.1.2.1.1 *** (gauge) 8
        🟢 Binding #2: enterprises.60000.1.2.1.2 *** (octet string) WIN7X64_DLADGLI
        🟢 Binding #3: enterprises.60000.1.2.1.3 *** (octet string) Log. Alert
        🟢 Binding #4: enterprises.60000.1.2.1.4 *** (octet string) C:\Documents\Research.docx
        🟢 Binding #5: enterprises.60000.1.2.1.5 *** (octet string) Rule: "Secret data" (Any keyword matched)
        🟢 Binding #6: enterprises.60000.1.2.1.6 *** (octet string) 2014-02-21T09:25:34Z
  
```

## Alerts Settings: SMTP

Use the **SMTP** tab in the **Alerts Settings** dialog box to configure e-mail notifications.

The image shows a Windows-style dialog box titled "Alerts Settings". It has four tabs: "SNMP", "SMTP" (which is selected), "Syslog", and "Delivery retry parameters". The "SMTP" tab contains three sections: "Connection" with fields for "SMTP host:" and "Port:" (set to 25); "Security" with a checkbox for "Server requires authentication", a "User name:" field, and a "Password..." button; and "Options" with "Sender address:" and "Recipients addresses:" text boxes. At the bottom, there is a "Threshold:" field set to 10, a unit dropdown menu set to "minute(s)", and a "Test" button. At the very bottom of the dialog are "OK", "Cancel", and "Apply" buttons. The "OK" button is highlighted with a red dashed border.

To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.
- Select **Alerts** in the console tree, and then click **Manage**  on the toolbar.
- Select **Alerts** in the console tree; then, in the details pane, right-click **SMTP** and click **Manage**.
- Select **Alerts** in the console tree, and then double-click **SMTP** in the details pane.

DeviceLock uses the Simple Mail Transfer Protocol (SMTP) for e-mail messaging. You can configure DeviceLock Content Security Server to automatically send notifications to the specified e-mail address(es) when alert conditions occur. To configure e-mail notifications, you'll have to specify SMTP server and configure e-mail notification settings.

Complete the **SMTP** tab as follows:

- **Connection** - Supply the mail sever-related information:
  - **SMTP host** - The name or IP address of the mail server.
  - **Port** - The port of the mail server. The default port is 25.

---

#### Note

Both non-SSL (unencrypted) and SSL connections to the mail server are supported. DeviceLock automatically identifies and sets the required connection type.

---

- **Security** - If the mail server requires authentication, select the check box **Server requires authentication**, and supply the name and password of the mail server user in the **User name** and **Password** name, respectively.
- **Options** - Define the mail sender and recipients:
  - **Sender address** - You can supply the address of the mail sender. Normally, this is the name of the mail server user, such as user@mailserver.com. The sender address appears in the **From** field of the e-mail message.
  - **Recipients addresses** - Specify the e-mail addresses of alert recipients (those who will receive the e-mail notification of events). Multiple addresses must be separated by a comma (,) or semicolon (;).
- **Threshold** - Specify the time interval (in hours, minutes or seconds) used for event consolidation when generating alerts. DeviceLock consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:
  - a. The events are of the same type, either **Success** for actions successfully performed on discovered content, or **Failure** for failed actions.
  - b. The **Reason** and **Computer** of the events being wrapped are the same.  
The default value is 10 minutes.
- **Test** - Click to send a test e-mail notification to verify that DeviceLock is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:
  - The test can complete successfully, meaning that a test e-mail notification was successfully sent using the configured e-mail notification parameters. The resulting message states: "Test SMTP alert was successfully sent."
  - The test can fail, meaning that a test e-mail notification was not sent. The resulting message states: "Test SMTP alert was not sent due to error: <error description>."

Below is an example of the e-mail alert.

### DeviceLock Alert

The following event has occurred:

Event type: Success (8)

Computer: WIN7X64\_DLADGLI

Date/Time: 02/21/14 12:05:02

Action: Log, Alert

Name: C:\Documents\Research.docx

Reason: Rule: "Confidential data" (Matched: All keywords)

---

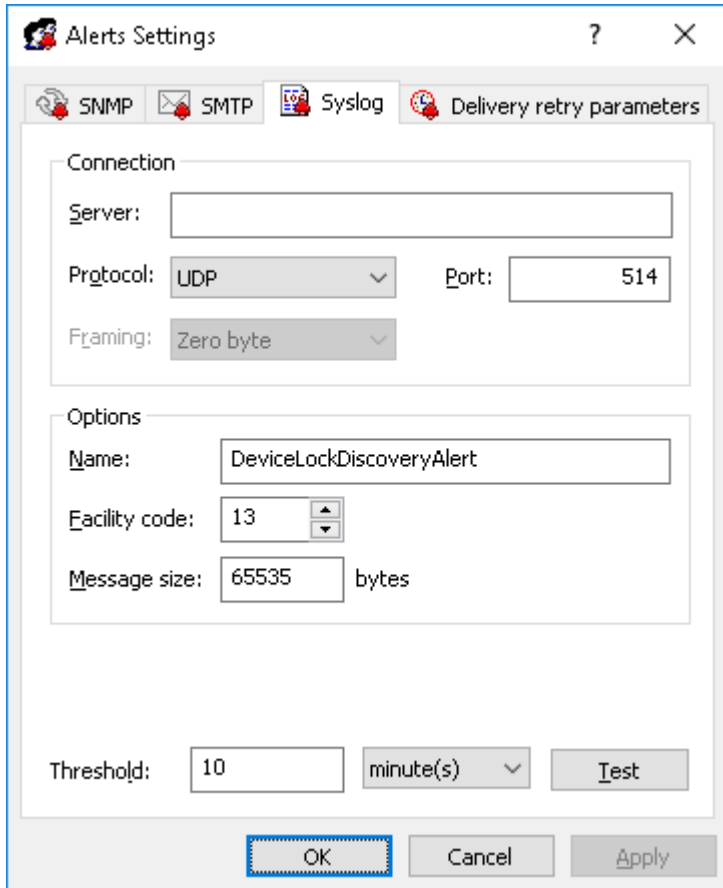
### Note

Field names in an e-mail alert correspond to the column names in the [Tasks Log Viewer](#).


---

## Alerts Settings: Syslog

Use the **Syslog** tab in the **Alerts Settings** dialog box to configure DeviceLock Content Security Server for syslog.

The image shows the 'Alerts Settings' dialog box with the 'Syslog' tab selected. The dialog has four tabs: 'SNMP', 'SMTP', 'Syslog', and 'Delivery retry parameters'. The 'Syslog' tab is active, showing two main sections: 'Connection' and 'Options'. In the 'Connection' section, there is a 'Server' text field, a 'Protocol' dropdown menu set to 'UDP', a 'Port' text field set to '514', and a 'Framing' dropdown menu set to 'Zero byte'. In the 'Options' section, there is a 'Name' text field set to 'DeviceLockDiscoveryAlert', a 'Facility code' spinner box set to '13', and a 'Message size' text field set to '65535' followed by the word 'bytes'. At the bottom of the dialog, there is a 'Threshold' section with a text field set to '10', a dropdown menu set to 'minute(s)', and a 'Test' button. At the very bottom are three buttons: 'OK', 'Cancel', and 'Apply'. The 'OK' button is highlighted with a blue dashed border.

To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.
- Select **Alerts** in the console tree, and then click **Manage**  on the toolbar.
- Select **Alerts** in the console tree; then, in the details pane, right-click **Syslog** and click **Manage**.
- Select **Alerts** in the console tree, and then double-click **Syslog** in the details pane.

You can configure DeviceLock Content Security Server to automatically send alert notifications to the specified syslog server when alert conditions occur. These alerts are sent only when all of the following conditions are met:

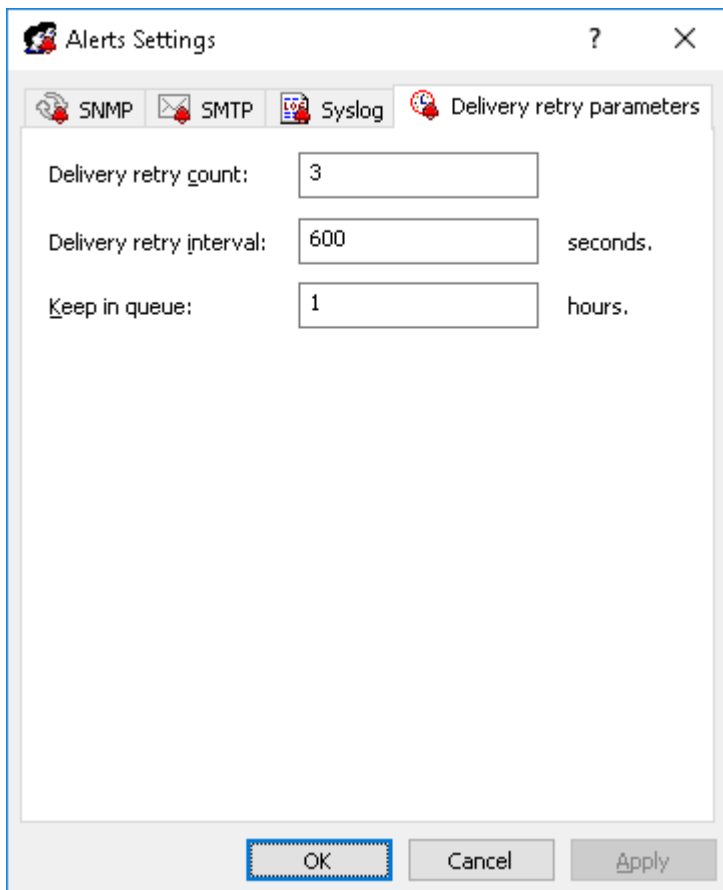
- The syslog server is set up to receive messages.
- The remote computer running the syslog server is accessible from computers where the discovery task is being performed (by the Agent) or from the server (in case of agentless scanning).
- Sending alerts to the syslog server is configured.

To configure sending alerts to the syslog server, complete the **Syslog** tab as follows:


- **Connection** - Supply the syslog server-related information:
  - **Server** - Specify the fully qualified domain name or IP address of the syslog server.
  - **Protocol** - Select **TCP** or **UDP** as the method of communication with the syslog server. The default selection is **UDP**.
  - **Port** - Specify the port number on which to send syslog messages. The default port is 514.
  - **Framing** - Specify the framing method for syslog messages when transported over TCP. DeviceLock supports these methods: **Zero byte**, **LF**, **CR+LF**, **Message length**.
- **Options** - View or change the following connection options:
  - **Name** - The unique name for the log channel. The default value is DeviceLockDiscoveryAlert.
  - **Facility code** - A syslog standard value (between 0 and 23) to specify the type of program that is logging the message.
  - **Message size** - The syslog message size, in bytes. The default value is 65535 bytes.
- **Threshold** - Specify the time interval (in hours, minutes and seconds) used for event consolidation when generating alerts. DeviceLock consolidates multiple similar events occurring within the threshold time and generates a summary in a single alert if all of the following conditions are true:
  - a. The events are of the same type, either **Success** for actions successfully performed on discovered content, or **Failure** for failed actions.
  - b. The **Reason** and **Computer** of the events being wrapped are the same.  
The default value is 10 minutes.
- **Test** - Send a test syslog message to verify that DeviceLock is configured correctly. This test operation can have two different outcomes, each resulting in a different message being displayed:
  - The test can complete successfully, meaning that a test message was successfully sent using the configured syslog parameters. The resulting message states: "Test Syslog alert was successfully sent."
  - The test can fail, meaning that a test message was not sent. The resulting message states: "Test Syslog alert was not sent due to error: <error description>."

## Alerts Settings: Delivery retry parameters

Use the **Delivery retry parameters** tab in the **Alerts Settings** dialog box to configure server actions in case of alert delivery failure.



To open this dialog box, do either of the following:

- Right-click **Alerts** in the console tree, and then click **Manage**.
- Select **Alerts** in the console tree, and then click **Manage**  on the toolbar.
- Select **Alerts** in the console tree; then, in the details pane, right-click **Delivery retry parameters** and click **Manage**.
- Select **Alerts** in the console tree, and then double-click **Delivery retry parameters** in the details pane.

DeviceLock generates and delivers alerts the moment the alert conditions are met. If alerts cannot be delivered on the first try, DeviceLock creates a queue to store undelivered alerts for a specified amount of time and sends them again. You can specify the maximum number of times DeviceLock attempts to send an alert, set the interval between delivery tries and also define the amount of time undelivered alerts are kept in the queue for delivery.

Complete the **Delivery retry parameters** tab as follows:

- **Delivery retry count** - Specify the maximum number of times DeviceLock attempts to send an alert if the first delivery attempt fails. If the first delivery attempt fails, the alert is deferred to the queue and marked as having had one delivery attempt. Thereafter, each time the queued alert is sent and delivery fails, the number of attempts is incremented.  
This parameter must contain a value between 0 and 1000. The default value is 3.

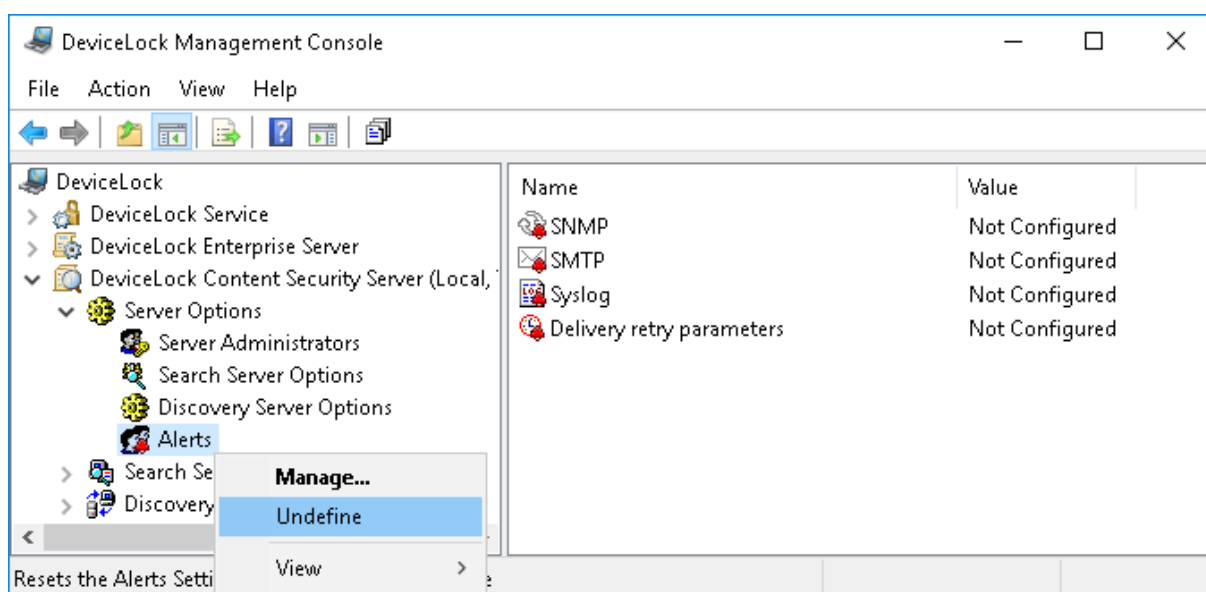
When the delivery retry count is reached and delivery fails, DeviceLock logs an error in the Discovery Tasks Log ("**<channel name>** for alerts is unavailable and temporary disabled due to error: **<error code>** - **<error description>**") and temporarily stops further transmissions through the alert delivery channel (SNMP, SMTP and/or syslog).

An attempt will be made to restore the delivery channel every time the agent successfully sends logs and status message to the Discovery Server.

- **Delivery retry interval** - Specify how many seconds DeviceLock waits before attempting next delivery of the alert, if the previous delivery failed. This parameter must contain a value between 10 and 3600. The default value is 600 seconds.
- **Keep in queue** - Define the amount of time in hours undelivered alerts are kept in the queue for delivery before they are deleted. The same queue is used for all delivery channels (SNMP, SMTP and/or syslog). This parameter must contain a value between 1 and 999. The default value is 1 hour.

## Resetting Alert Settings to Defaults

At any time you can reset alert settings to their default state ("undefined"). To undefine all alert settings, right-click **Alerts** in the console tree, and then click **Undefine** on the shortcut menu. This command resets the alert settings to their default ("undefined") state.



## Resetting Individual Settings

You can also undefine individual options such as **SNMP**, **SMTP**, **Syslog** and **Delivery retry parameters**. In order to undefine any of these options, select **Alerts** in the console tree, and then right-click individual items appearing in the details pane. Click **Undefine** on the shortcut menu to reset the selected parameter.



# Endpoint Scanning

## Discovery Server

Discovery Server scans user computers and data stores, applying configurable rules to discover certain content. Scanning can be accompanied by various actions depending upon the discovery settings, for example, it can grant or deny access to content, delete or encrypt content, alert administrators, or notify computer users.

The basis of the discovery settings is the so-called “units” that determine the scan area. This area can be configured to include local computer disks and folders, as well as SMB network shares. Units are assigned discovery rules along with the actions to perform when content matching those rules is discovered.

After configuring units, rules, and actions, the administrator can set up and run discovery tasks. When running, such a task scans its units, and applies the rules and actions specified. In addition, the task creates reports and logs events, making it possible to view and analyze the results of discovery and the actions performed.

The discovery setup procedure can be summarized as follows:

1. Configure units, specifying the data locations to scan. For details, see [Units](#).
2. Configure discovery rules along with the actions to be performed upon content discovery. For details, see [Rules and Actions](#).
3. Configure discovery tasks, and schedule them to run. For details, see [Tasks](#).

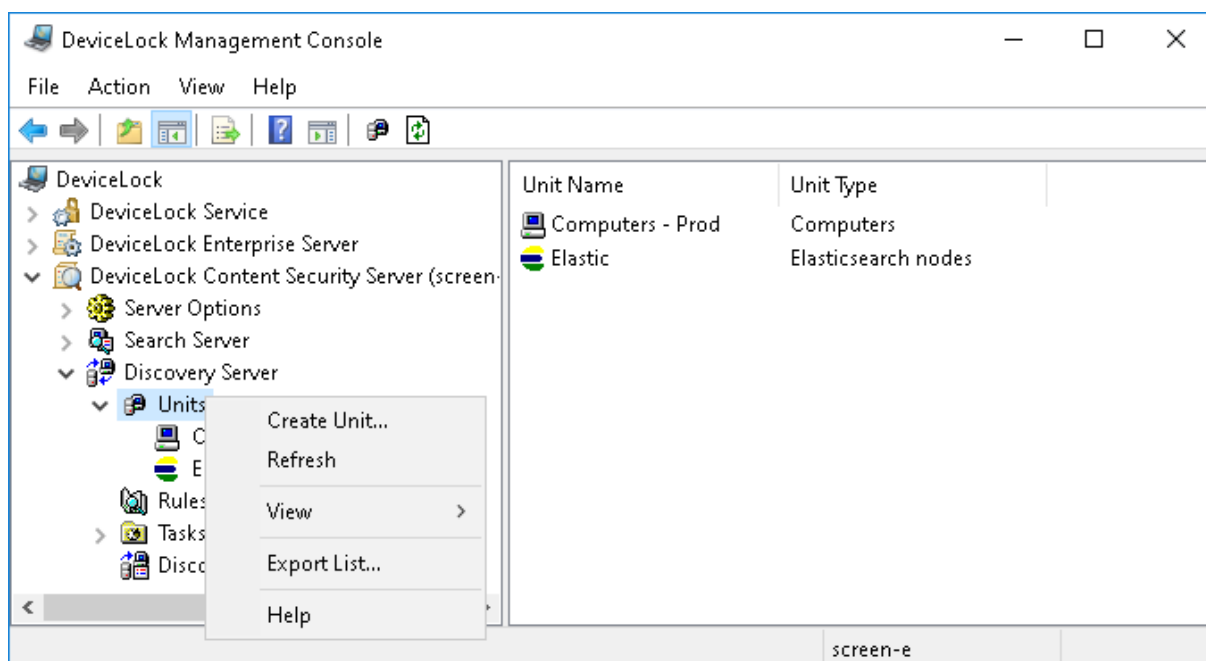
## Units

In DeviceLock Discovery, a unit is a basic entity for the purpose of content discovery. A unit is composed of one or more computers with either of the following properties:

- Common credentials.
- Common scanning area settings (defined by using Include and Exclude filters).
- Common scanning type.

All units that currently exist on the server are listed in the console tree under **DeviceLock Content Security Server > Discovery Server > Units**.

When you select the **Units** node in the console tree, the details pane lists the units that currently exist on the server.



The list in the details pane displays the following information on each unit:

- **Unit Name** - The name that identifies the unit.
- **Unit Type** - Intended use of the unit: scan computers (**Computers** unit type) or scan Elasticsearch nodes (**Elasticsearch nodes** unit type).

The shortcut menu on the **Units** node includes the following commands:

- **Create Unit** - Creates a new unit. You can specify the desired settings for the new unit in the dialog box that appears when you select this command.
- **Refresh** - Updates the list of units with the latest information.

The shortcut menu on a unit in the details pane includes the following commands:

- **Edit Unit** - Opens a dialog box where you can view or change the settings of the selected unit.
- **Duplicate Unit** - Creates a new unit with the settings copied from the selected unit. You can view or change the settings of the new unit in the dialog box displayed by this command. By default, the new unit name consists of the **Copy of** prefix followed by the name of the selected unit. When you create two or more copies of a unit, the new unit name includes a numeric suffix indicating the number of the copy.
- **Edit Computers List** - Opens a dialog box where you can view or change the list of computers included in this unit.
- **Delete Unit** - Deletes the selected unit.
- **Refresh** - Updates the list of units with the latest information.

## Creating a Unit

To create a unit, open and complete the **Create Unit** dialog box. You can open that dialog box as follows:

1. In the console tree, expand **DeviceLock Content Security Server > Discovery Server > Units**.
2. Right-click the **Units** node, and then click **Create Unit** on the shortcut menu.  
- OR -  
Select the **Units** node, and then click **Create Unit** on the toolbar.

The **Create Unit** dialog box appears.

**Create Unit**

Name:

Unit type:

Computers:

Include Filter(s)

Drives	Paths	Files
All	All	All

Exclude Filter(s)

Drives	Paths	Files
'Network' OR 'Remo...	All	All

☐ Agentless Discovery

☐ Install Discovery Agent automatically

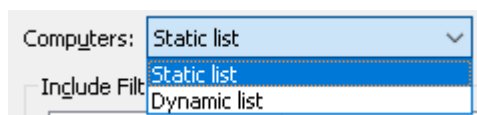
☐ Remove Discovery Agent automatically

Complete the **Create Unit** dialog box as follows:

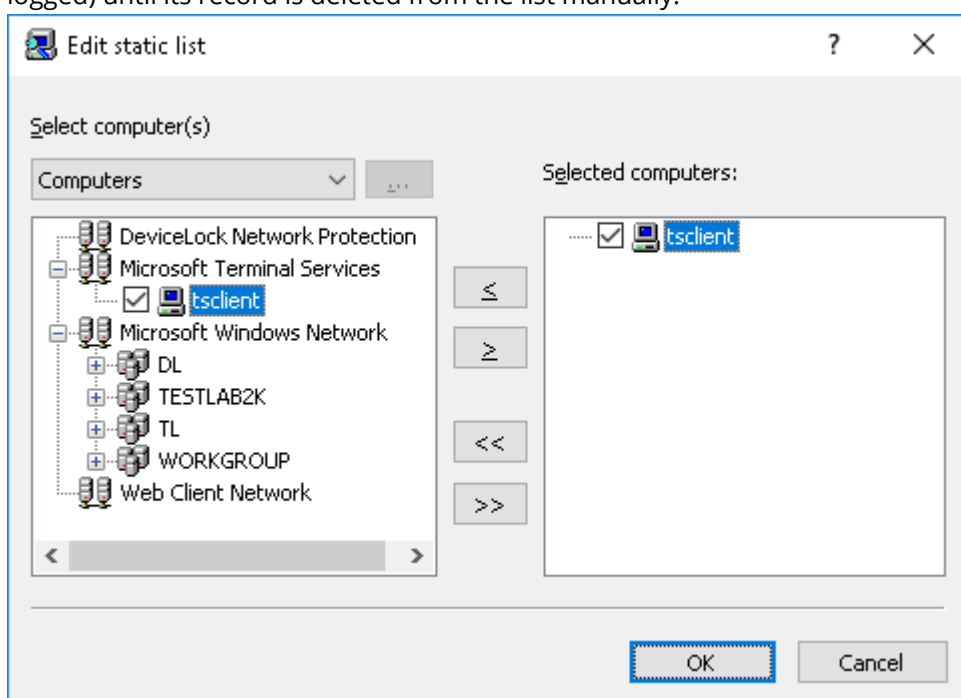
- **Name** - Specify a display name for the newly created unit.
- **Unit type** - To discover files on computers and servers, choose the **Computers** unit type. Choose the **Elasticsearch nodes** unit type for document discovery in Elasticsearch.

This section describes the **Computers** unit type. For description of the **Elasticsearch nodes** unit type, see [Elasticsearch Units](#).

- **Computers** - Specify the computer list for this unit. There are two list types: **Static list** and **Dynamic list**. You can choose the type of the list when creating a unit. Thereafter the list type cannot be changed.



1. **Static list** - All computers are specified in the list by their names or IP addresses. Since this list is static, even if some computer no longer exists in the network, it will be scanned (and the error logged) until its record is deleted from the list manually.

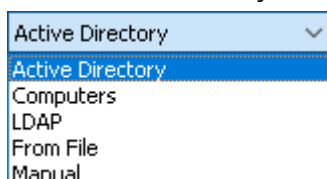


Computers that will be scanned must be specified in the list on the right. Select computers from the list on the left, and then move them to the list on the right by clicking the **>** button.


If you need to exclude some computers from the scanning job, select them in the list on the right and click the **<** button.

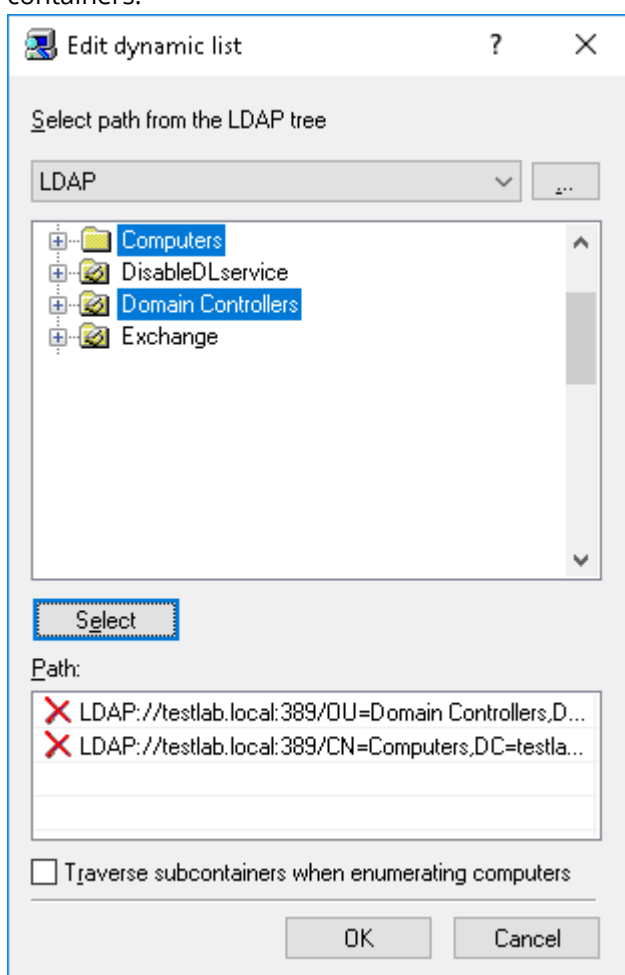
By using the **>>** and **<<** buttons, you can add and remove all available computers at the same time (no need to select computers in the list).

There are several ways to choose network computers from the left-hand list:



- **Active Directory** - Select computers from Active Directory folders (organizational units).
- **Computers** - Select computers that exist on the network.

- **LDAP** - Select computers from an LDAP-compatible directory.
  - **From File** - Load a list of computers from a text file and then select computers. To open a text file, click the  button. In the file, each computer's name or IP address must be on a separate line.
  - **Manual** - Type computer names manually to select the computers. Press ENTER as needed to type each computer's name or IP address on a separate line.
2. **Dynamic List** - Instead of computer names or IP addresses, you may specify a dynamic list containing path to the container (for example, an organizational unit) in the directory service tree such as Active Directory, Novell eDirectory, OpenLDAP and so on. Every time the task is executing, Discovery Server retrieves all the computers that currently exist in that container. Hence, if some computer was removed from the directory tree or moved to another container it will not be scanned anymore. And vice versa, if there is some new computer that did not exist in the container at the time the task was created/ modified, but was added to this container later, it will be retrieved and scanned at the time of executing the task. You can select one or more containers.



The path to the selected containers is specified in the **Path** field. Select containers in the tree by clicking while holding down the Shift or Ctrl key. Then click the **Select** button. To deselect the container, click the red X in the **Path** field.

Select the **Traverse subcontainers when enumerating computers** check box to allow Discovery Server to retrieve computers from all the nested containers located inside the selected container. Otherwise, if this check box is cleared all nested containers are ignored, and only computers located directly in the selected container are retrieved at the time of executing the task.

There are two modes to work with the directory service:

- **Active Directory** - You browse the Active Directory tree and select the needed container. While the Active Directory tree can also be displayed by choosing the **LDAP** option (see below), the Active Directory mode results in greater efficiency between the directory service and DeviceLock Discovery Server and thus resource savings. If you need to supply alternative credentials to access Active Directory, click the **...** button and specify the needed user account and its corresponding password.

---

**Note**

If no alternative credentials are specified when accessing Active Directory, DeviceLock Discovery Server uses the credentials of the account under which the DeviceLock Content Security Server service is started. For more information, see [Setting the service startup account](#).

---

Select the **Synchronization** check box to allow DeviceLock Discovery Server to use the synchronization feature of Active Directory. This will dramatically reduce the load on the domain controller and speed up the process of retrieving computers at the time of task execution.

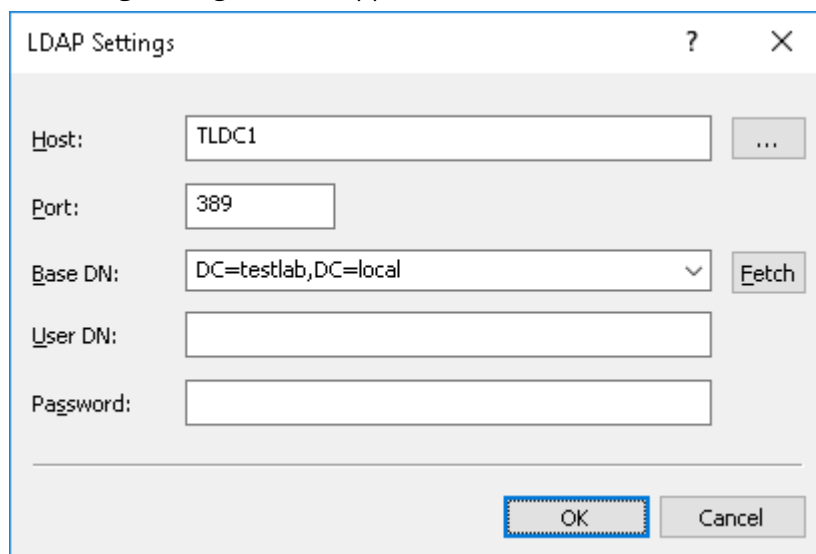
---

**Note**

To use the synchronization feature, DeviceLock Discovery Server must have access to Active Directory with domain administrator rights.

---

- **LDAP** - You browse the LDAP (Lightweight Directory Access Protocol) tree and select the needed container. To configure a connection to the LDAP server, click the **...** button and complete the **LDAP Settings** dialog box that appears.



The image shows a screenshot of the 'LDAP Settings' dialog box. The dialog has a title bar with a question mark and a close button. It contains several input fields: 'Host' with the value 'TLDC1' and a browse button (...), 'Port' with the value '389', 'Base DN' with a dropdown menu showing 'DC=testlab,DC=local' and a 'Fetch' button, 'User DN' with an empty text box, and 'Password' with an empty text box. At the bottom, there are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a blue dashed border.

- **Host** - The name or the IP address of the LDAP server to connect to.
- **Port** - The TCP port on which the LDAP server accepts connections. The default port is 389.
- **Base DN** - The starting point to search the directory tree. This must be a valid distinguished name (DN), such as `cn=users,o=company,c=US`. If the base DN is not specified, the search goes from the tree root. Click the **Fetch** button to select a naming context for the base DN.
- **User DN, Password** - The distinguished name (DN) and password of the directory user to access the LDAP server. User DN must be a valid DN, such as `cn=admin,o=company,c=US`.

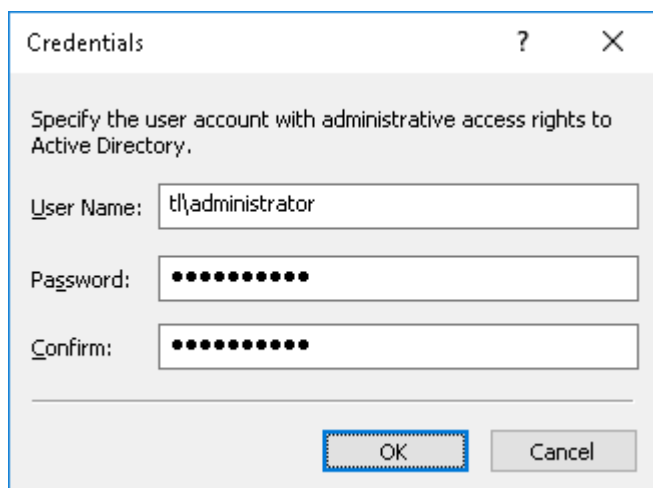
---

#### Note

If no user DN is specified, Discovery Server uses the credentials of the DeviceLock Content Security Server service's startup account. For more information, see [Setting the service startup account](#).

---

- **Set Credentials** - Optionally, click to specify the name and password of the user account with sufficient rights to access the listed computers. It is advisable to choose an account with administrative rights on all those computers.



Setting credentials is optional. If no credentials are set, Discovery Server accesses remote resources with the DeviceLock Content Security Server service's startup account, or uses the DeviceLock Certificate to access the DeviceLock Service with a Certificate installed.

---

#### Note

- In order to apply the specified credentials, the DeviceLock Content Security Server service's startup account must be an account with local administrator rights.
  - If using a database from another Discovery Server, you will need to re-enter the credentials. Since credentials are encrypted with a key securely stored on the server, they cannot be decrypted by another Discovery Server, so they must be re-entered.
- 

- **Include Filter(s) / Exclude Filter(s)** - Use include and exclude filters to specify which disks, folders and files you want the server to scan. By default, DeviceLock Discovery will scan all disks, files and folders except removable and network devices.

Click **Add** under corresponding filter list to create a new filter. The **Add Exclude Filter** dialog will appear when adding an exclude filter. The **Add Include Filter** dialog appears when adding an include filter. For details, see [Adding Filters](#). You can also change or delete filters by clicking the **Edit** or **Delete** button, respectively.

The rules in each filter are combined by OR logic. For example, if an include filter has the **System**, **Non-system** and **Removable, Floppy & Optical** check boxes selected, then only devices of these types will be scanned. If, in addition, you select the **Documents** check box, then only the Documents folder will be scanned on the selected device types. If you specify multiple filters, they will be combined by OR logic, i.e. the scanning area includes the items that match any of the filters. Include and exclude filters are combined by AND logic. See also [Creating a filter: Example](#).

- **Agentless Discovery** - Select this check box if you want the server to scan remote computers without using Discovery Agent. The Agent is not installed on remote systems, and the scanning is performed via the SMB protocol. Depending on specified detection rules, the full content of the files being analyzed may be required. If this is the case, the files being analyzed will be transferred to the server for analysis, which may consume large amounts of bandwidth.
- **Install Discovery Agent automatically** - Select this check box if you want the server to install the Discovery Agent on the remote system if one is not yet installed, or if the remote system is not running DeviceLock Service with its bundled Discovery Agent.
- **Remove Discovery Agent automatically** - Select this check box if you want the server to remove the Discovery Agent from remote systems after the scanning task completes. Note that this option does not cause the server to remove DeviceLock Service and its bundled Discovery Agent.

---

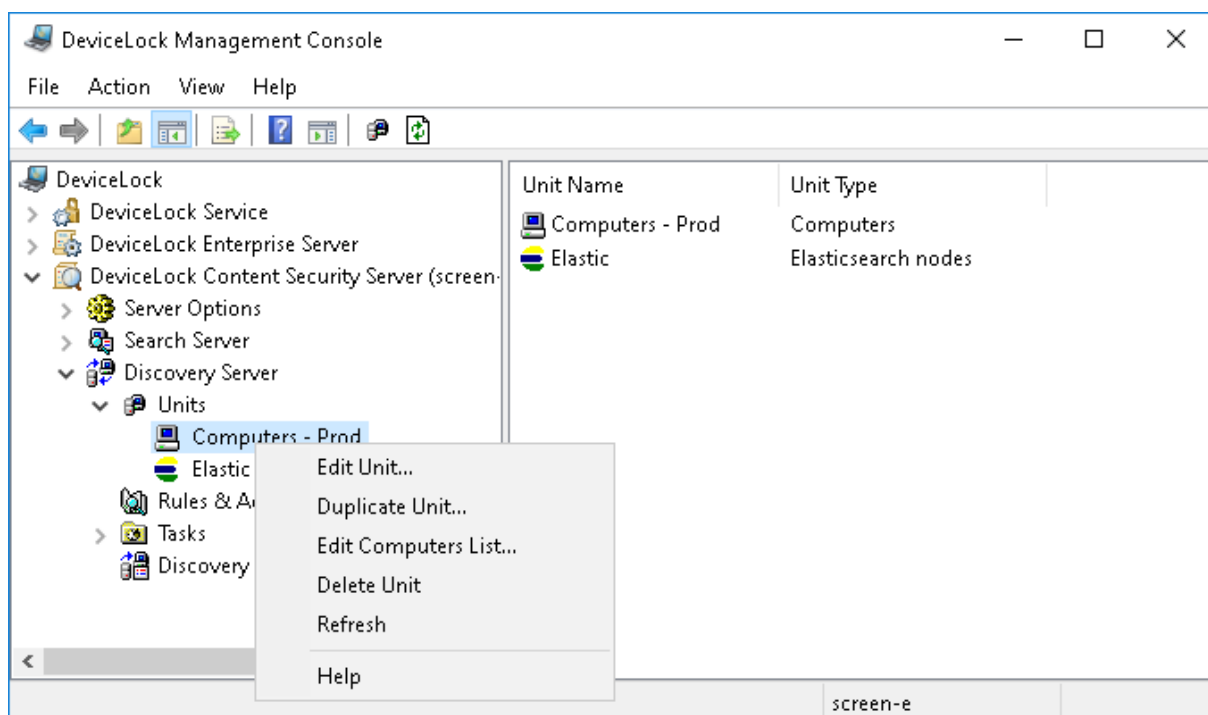
**Note**

If the DeviceLock Content Security Server service is configured to run under the Local System account, Discovery Server cannot install or remove Discovery Agents on remote computers.

---

The unit you have created appears in the console tree:





## Adding Filters

This section describes how to configure filters for a Computers unit. To configure filters for an Elasticsearch unit, see [Filter control dialog box for Elasticsearch](#).

To add a filter, use the **Add Include Filter** or **Add Exclude Filter** dialog box depending on the type of the filter.

**Add Include Filter**

☐ All Drives (not available for agentless discovery)

☒ System ☐ Network

☒ Non-system ☒ Removable, Floppy & Optical

☐ All Paths

Predefined

☒ Documents ☒ System Folder

☒ Program Files ☒ Temporary Folder

Cloud storage folders:

Custom

Path:

☐ Including Subfolders

☐ All Files

File name:

Modified:  1/ 1/2020 12:00 PM  1/ 1/2020 12:00 PM

File size:  0  0 bytes

Attributes

☐ System ☐ Hidden ☐ Encrypted

**OK** Cancel

Complete this dialog box as follows.

1. Specify the drives to include or exclude:

- **All Drives** - Allows you to specify the types of storage devices to scan. These parameters are not supported in Agentless mode, in which case all disks will be scanned regardless of their type.

---

#### Note

If the **All Drives** option is selected, the check boxes described below have no effect and the filter will include or exclude all disks.

---

- **System** - Select to specify the logical disk where Windows is installed.
- **Non-system** - Select to specify all other logical and physical disks that do not fall to other classifications.

- **Network** - Select to specify mounted network disks. Multiple networks disks may exist for each logged in user. All network disks for all users will be scanned.
  - **Removable, Floppy & Optical** - Select to specify removable disks including floppy drives, optical drives (CD/DVD/BD-ROM). This also includes USB pen drives, attached memory cards, external storage devices connected via a USB cord etc.
2. Specify the paths to include or exclude:
- **All Paths** - Allows you to specify the paths on the disks to scan.

---

**Note**

If the **All Paths** option is selected, the check boxes described below have no effect and the filter will include or exclude all paths.

---

- **Documents** - Select to specify the Documents folder. On systems earlier than Windows Vista, the path to this folder is %SystemDrive%\Documents and Settings\<user>\My Documents. On Windows Vista or later, the path is %SystemDrive%\Users\<user>\Documents. Document folders are scanned for every users.
- **Program Files** - Select to specify the Program Files folder. On 64-bit systems, both Program Files and Program Files (x86) will be scanned.
- **System folder** - Select to specify the Windows installation folder.
- **Temporary Folder** - Select to specify the system temp folder.
- **Cloud storage folders** - Select to specify whether to scan the user's local synchronization directories for selected cloud storage services. The following services are supported: Amazon Cloud Drive, Box, Cloud Mail.ru, Copy, Dropbox, Google Drive, iCloud, MediaFire, OneDrive, SpiderOak, SugarSync, Yandex.Disk.

---

**Note**

The user (the owner of local synchronization directory) must be logged in for the **Box** cloud storage service directory to be scanned.

---

- **Path** - Enter custom paths to scan. Multiple paths can be specified by using a semicolon (;) as a delimiter. UNC paths (e.g. \\server\share) are supported. You can use wildcards, such as asterisks (\*) and question marks (?).  
See also [Scanning a network share: Example](#).
  - **Including subfolders** - Specify whether to scan subfolders within the previously defined paths. If this option is not selected, only the files located in the specified folder will be scanned.
3. Specify the files to include or exclude:
- **All Files** - Allows you to specify the files to include or exclude.

---

**Note**

If the **All Files** option is selected, the check boxes described below have no effect and the filter will include or exclude all files.

---

- **File name** - Specify the desired file names. Multiple file names must be separated by a semicolon (;); for example, \*.doc; \*.docx.  
You can use wildcards, such as asterisks (\*) and question marks (?). An asterisk matches any series of characters or no characters. For example, \*.txt matches any file name with the extension of txt. The question mark matches any single character. For example, ????.\* matches any file name composed of 4 characters and any extension.
- **Modified** - Specify the desired last modification date/time of the file. To do so, choose from the following options in the **Modified** drop-down list:
  - **Not specified** (this option is selected by default).
  - **Before than** - The file's modified date/time must be earlier than the specified date/time.
  - **After than** - The file's modified date/time must be later than the specified date/time.
  - **Between** - The file's modified date/time must fall within the specified date/time range.
  - **Not older than** - The file's modified date/time must not be older than the specified number of seconds, minutes, hours, days, weeks, months, or years.
  - **Older than** - The file's modified date/time must be older than the specified number of seconds, minutes, hours, days, weeks, months, or years.
- **File size** - Specify the desired file size in bytes, kilobytes, megabytes, gigabytes or terabytes. To do so, choose from the following options in the **File size** drop-down list:
  - **Not specified** (this option is selected by default).
  - **Equal to** - The file must be exactly the specified size.
  - **Less than** - The file must be smaller than the specified size.
  - **More than** - The file must be larger than the specified size.
  - **Between** - The size of the file must fall within the specified range.
- **Attributes** - Specify the desired file attributes. The **System**, **Hidden** and **Encrypted** attributes are directly matched to the corresponding NTFS attributes.

## Creating a filter: Example

This example shows how to configure filters to scan any removable drives (including all currently inserted USB pen drives) as well as the folder D:\Custom\.

In order to create such a unit, two Include filters must be specified, one enabling the scanning of all removable drives, and the other enabling the scanning of the custom folder. If we were to create a single filter combining both scanning parameters, the logical AND operator would be applied, and such filter would only enable the scanning of the D:\Custom\ folder located on removable drives.

Create the first Include filter to scan any removable drives:

- Clear the **All Drives** check box and all check boxes in this category.  
Select the **Removable, Floppy & Optical** check box.
- Select the **All Paths** check box.
- Select the **All Files** check box.

Create the second Include filter to scan the folder D:\Custom\:

- Select the **All Drives** check box.
- Clear the **All Paths** check box and all check boxes in this category.  
Enter D:\Custom\ in the **Path** field under **Custom**.
- Select the **All Files** check box.

## Scanning a network share: Example

Suppose you need to scan a network share on a server or NAS device with an operating system on which DeviceLock cannot be installed (for example, a Linux OS). The network share is identified by a UNC path, such as \\server\share.

You can perform this task by configuring a unit as follows:

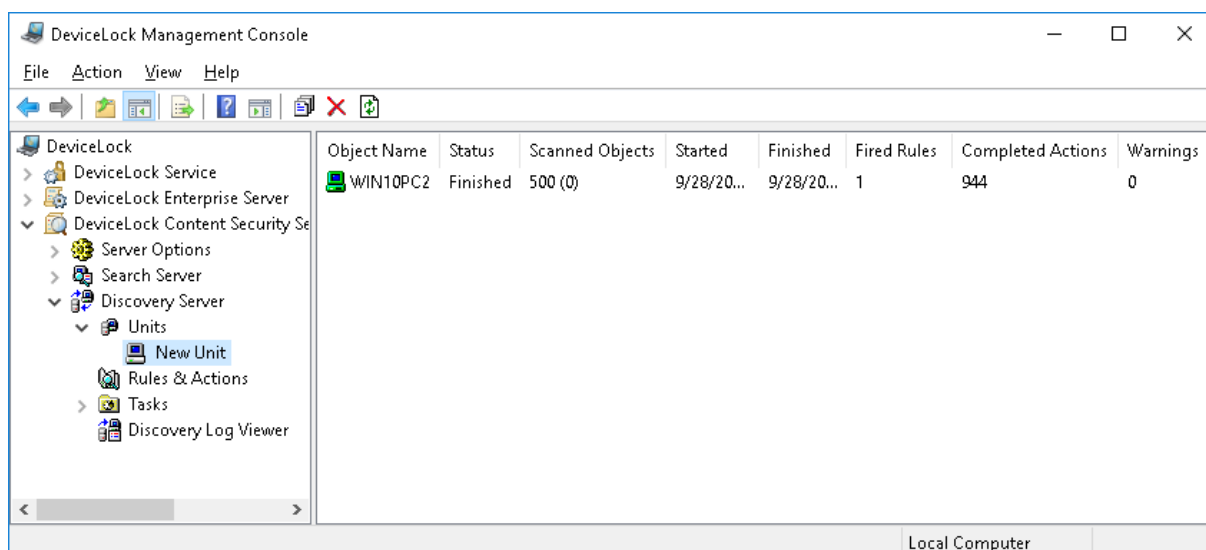
- Add a computer to the unit from which the network share can be accessed. This can be the computer running Discovery Server, or another computer with an operating system that allows DeviceLock installation (such as a Windows OS). For instructions, see [Creating a Unit](#).
- Ensure that the user account under which Discovery Server performs a scan on that computer has sufficient rights to access the network share. At least read access is required. If during the scan Discovery Server needs to make changes on the network share (for example, encrypting files or setting permissions), appropriate access rights will be required.  
If the user account used by default to perform the scan does not have sufficient rights to access the network share, configure the unit to use alternative credentials. In the dialog box for creating or editing the unit, click the **Set Credentials** button, and specify the name and password of the user with the required access rights.
- Add an include filter to the unit. In the **Path** field of the filter, specify the UNC path of the network share.

Configure content discovery rules (see [Rules and Actions](#)), set up a discovery task based on the unit and rules you have configured (see [Tasks](#)), and run the task to perform the desired scan.

## Managing Units

The console displays units in the console tree under **DeviceLock Content Security Server > Discovery Server > Units**.

When you select a unit in the console tree, the details pane displays the contents of that unit:



The details pane lists the following information about each computer held in the selected unit:

- **Object Name** - The name that identifies the computer.
- **Status** - The computer's status. The status can receive one of the following values:
  - **Waiting** - The computer is waiting for the scanning task to be run on that PC. This status is assigned when the applicable Task receives the status of **Running**.
  - **Scanning** - The computer is currently being scanned.
  - **Finished** - Indicates successful completion of the scanning task. The scanning of the computer has successfully completed.
  - **Expired** - Indicates a problem that impedes a scan task. The computer became unavailable during the execution of the task (for example, the computer has disconnected from the network, the network settings have changed, or some other problem did not allow the Discovery agent to transfer data to the server), and the computer did not respond for the period of time specified by the [Keep-alive timeout](#) parameter. The **Expired** status is also assigned if the scan task takes longer than specified by the [Stop task if runs longer than](#) parameter, which forces it to terminate prematurely.
  - **Access is denied** - Indicates a problem accessing the resource (e.g. computer). This can mean that the unit's specified credentials did not work (certificate or startup account error depending on configuration).
  - **Installation failed** - Indicates there was a problem installing Discovery Agent.
  - **No License** - Indicates that you don't have enough licenses to scan the computer.
  - **Canceled** - Indicates that the scanning task is being canceled.
  - **Canceled** - Indicates that the task has been canceled.
  - **Computer is unavailable** - Indicates that either of the following issues has occurred after the number of attempts specified by the [Number of retries](#) parameter or on the expiry of the time period determined by the [Retry timeout](#) parameter:
    - Failed to connect to a remote computer in order to begin scanning (in agentless mode).
    - Failed to connect to a remote computer and communicate the scanning task to the Discovery agent. This can happen because the computer was unavailable (e.g. turned off or

not connected to the network), or the Discovery agent was not installed or launched on that computer while the agent installation setting is not enabled in the unit properties (the **Install Discovery Agent automatically** flag is not set).

- **Scanned Objects** - Indicates the total number of scanned objects. The value in parentheses indicates the number of scanned nested objects.  
Example: "1 (20)" means 1 container (archive) with 20 files inside.  
For each unit, the list counts and displays the total number of objects inspected during the most recent scan of that unit. The counter of scanned objects is reset each time a new scan of the unit starts. The same applies to other counters in this list.  
For Elasticsearch units, scanned objects are document fields rather than documents. The counter of scanned objects displays the total number of fields inspected when scanning the Elasticsearch unit.
- **Started** - Indicates the date and time when the server started scanning the unit.
- **Finished** - Indicates the date and time when the server finished scanning the unit.
- **Fired Rules** - The number of different rules that discovered a match. If a certain rule discovered more than one match, it will be still counted as 1.
- **Completed Actions** - Indicates the number of actions performed during the scan.  
Example: If a rule discovers a match, deleted a file, logged the event and sent a notification, this will count as 3 actions.
- **Warnings** - Indicates the number of scanning errors. This counter is increased if a matching object was discovered but it was impossible to take an action, or if content analysis was impossible (e.g. an attempt to analyze a corrupted or password-protected archive).

The shortcut menu on a unit in the console tree includes the following commands:

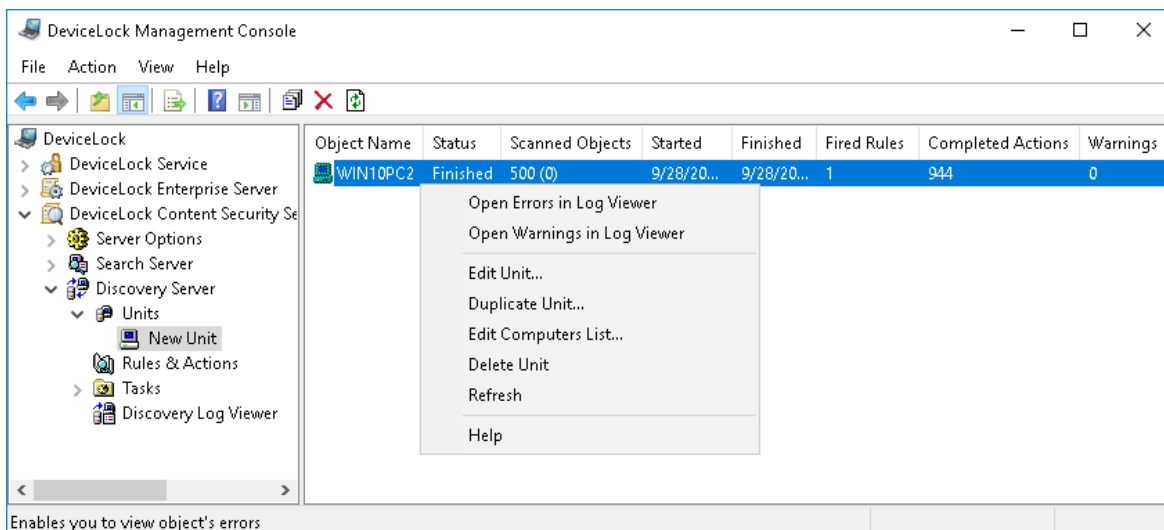
- **Edit Unit** - Opens a dialog box where you can view or change the settings of the selected unit.
- **Duplicate Unit** - Creates a new unit with the settings copied from the selected unit. You can view or change the settings of the new unit in the dialog box displayed by this command.  
By default, the new unit name consists of the **Copy of** prefix followed by the name of the selected unit. When you create two or more copies of a unit, the new unit name includes a numeric suffix indicating the number of the copy.
- **Edit Computers List** - Opens a dialog box where you can view or change the list of computers included in this unit.
- **Delete Unit** - Deletes the selected unit.
- **Refresh** - Updates the list in the details pane with the latest information.  
Since the console does not automatically update information displayed in the details pane, you need to update the list by using the **Refresh** command.

You can use the shortcut menu to manage computers held in the unit. To open the menu:

1. Expand **DeviceLock Content Security Server > Discovery Server > Units** in the console tree.
2. In the list under the **Units** node in the console tree, click the unit you want to manage.  
*A list of computers will appear in the details pane.*

3. Right-click a computer in the details pane.

*The shortcut menu will appear.*



The shortcut menu on a computer in the details pane includes all commands that appear on the shortcut menu of the unit selected in the console tree as well as the following commands that apply to the selected computer:

- **Open Errors in Log Viewer** - Opens the Log Viewer with pre-defined filter settings to only display scanning errors for the selected computer. All errors occurred in all tasks and during the entire period of time will be displayed.
- **Open Warnings in Log Viewer** - Opens the Log Viewer with pre-defined filter settings to only display scanning warnings for selected computer. All warnings occurred in all tasks and during the entire period of time will be displayed.

## Elasticsearch Units

DeviceLock Discovery can effectively discover documents of interest in Elasticsearch - a distributed system that provides real-time indexing and search for a wide variety of data types. The Discovery Server requests a document search by the specified configurable parameters, and then applies the discovery rules and actions to documents received from Elasticsearch. Discovery rules are matched to data in the document fields selected in accordance with filter settings (see [Filter control dialog box for Elasticsearch](#)). The rule triggers if it matches data in at least one of those fields.



---

### Important

- DeviceLock supports document discovery in Elasticsearch version 6.8.12 or later.
  - Document discovery in Elasticsearch requires one DeviceLock Discovery license for each Elasticsearch index that will be searched for documents.
  - The DeviceLock Discovery agent is not installed on Elasticsearch nodes. Discovery is performed without the use of the agent.
  - Elasticsearch-related discovery actions are limited to logging events and sending alerts. The Discovery Server cannot change or delete documents in Elasticsearch.
-



To interact with Elasticsearch, a discovery task must use a unit of the appropriate type: when creating such a unit, select **Elasticsearch nodes** in the **Unit type** list. The following parameters are used to configure a unit of this type:

- **Computers** - A configurable list of computers running Elasticsearch nodes that are subject to discovery. Click the **Edit** button next to the **Computers** field, and then, in the dialog box that appears, view the current list, and add or remove computer names from this list as needed. The names of computers running the desired Elasticsearch nodes are listed in the right pane of the dialog box. To add computer/s to the list, type their name/s or IP address/es in the left pane and click the  button. You can type the host name or fully qualified domain name (FQDN) of the computer. Press ENTER after typing each name. To remove computer/s, select their name/s in the right pane and click the  button.

When typing a computer name, you can specify the number of the network port used by Elasticsearch, in the format name:port. If the port is not specified, the discovery task will scan all ports until it detects Elasticsearch. To speed up port scanning, select the **Smart port lookup** check box. When this check box is selected, the discovery task will only scan ports that are typically used by Elasticsearch. As port search can be time consuming, it is advisable to specify the Elasticsearch port number explicitly.

- **Set Credentials** - Click this button to specify the name and password of a user account with sufficient rights to access the Elasticsearch nodes on the servers in this unit. A name and password must be specified if Elasticsearch requires authorized access. If no account name and password are specified, the Discovery Server accesses Elasticsearch anonymously.

---

**Note**

If using a database from another Discovery Server, you will need to re-enter the account name and password. Since these credentials are encrypted with a key securely stored on the server, they cannot be decrypted by another Discovery Server, so the name and password must be re-entered.

---

- **Include Filter(s)** - Conditions for including indexes and documents in the discovery process. The search is conducted only by indexes and documents that match at least one of these filters. Use buttons beneath this field to add, edit, or delete include filters. When adding or editing a filter, the [Filter control dialog box for Elasticsearch](#) is used.
- **Exclude Filter(s)** - Conditions for excluding indexes and documents from the discovery process. The search is not conducted by indexes and documents that match any of these filters. Use buttons beneath this field to add, edit, or delete exclude filters. When adding or editing a filter, the [Filter control dialog box for Elasticsearch](#) is used.
- **Query <number> documents** - Select this check box to specify the maximum number of documents to be requested from Elasticsearch. During the discovery process, Elasticsearch will return no more than the specified number of documents that match the filters in effect. Clear this check box if you want Elasticsearch to return all documents that match the filters.
- **Sorting** - The sort order of the documents returned by Elasticsearch. Clear the **Sort by** check box if it does not matter in which order the documents arrive from Elasticsearch (default sorting). Select this check box to have documents arrive in ascending or descending order of values of a

certain field in the document. Specify the name of that field in the **Field** box, and select the desired sort order (**ascending** or **descending**).

---

**Note**

The same field can be indexed in different ways for different purposes (so-called *multi-field*). For instance, a string field could be mapped as a text field for full-text search, and as a keyword field for sorting and aggregations. In this case, it is advisable to specify the field for sorting as `fieldname.keyword`.

---

The fields that list the filters display the following conditions for each filter:

- **Index** - A list of index names. The filter matches documents from any of the listed indexes. Index names allow the use of wildcards: an asterisk (\*) stands for an arbitrary series characters, a question mark (?) stands for any single character. For instance, a dot followed by an asterisk (.\*) denotes any index whose name begins with a dot.

The condition of All indicates that the filter matches documents from any index.

- **Field : Value / Query** - A list of field-value pairs or a search query. In this filter condition, "Field" stands for the name of the field in Elasticsearch documents and "Value" stands for the value to search for in the field specified. "Query" stands for a query string that complies with Elasticsearch query syntax.

If a list of field-value pairs is specified, the filter matches documents in which the specified fields have the specified values. If a query string is specified, the filter matches the documents returned by the respective search query.

In a field-value pair, <All values> indicates that the filter matches documents with any value in the field specified.

The <All> mark indicates that the filter matches any documents from the indexes specified.

Index names that begin with a dot normally denote system indexes (for example, .kibana). As such indexes hold configuration settings and other system data, it is advisable to exclude them from the discovery process. Therefore, the exclude filter has the following default conditions: Index = .\*; Field : Value / Query = All, which excludes all documents in all indexes whose names begin with a dot.

## Filter control dialog box for Elasticsearch

filters specify the search parameters for documents in Elasticsearch, and determine the document fields to discover. Discovery rules are applied to indexes and documents that match include filters and do not match exclude filters. Discovery rules inspect the fields specified by include filter settings (see [Fields](#) for details).

The filter control dialog box is used when adding or editing a filter. It provides the following filter condition controls:

- [Indexes](#) - Filtering by document location.
- [Fields](#) - Filtering by document field data.

### **Indexes**

Select the **All indexes** check box if you want documents from any index to match the filter. Clear this check box if you need to specify indexes explicitly. As a result, only documents from indexes whose names are listed in the **Index** field will match the filter.

In the **Index** field, one can enter multiple names separated by semicolons (;), as well as use wildcards: an asterisk (\*) for an arbitrary series characters, a question mark (?) for any single character.

To help configure filters, the **Index** field remembers previously entered names, and allows them to be selected from the drop-down list.

### **Fields**

Select the **All documents** check box if you want any documents from the specified indexes to match the filter. Clear this check box if you need to filter documents by their field values or by using a search query. As a result, the filter will match only documents matching each of the specified field-value pairs (option **Custom**) or those returned by the specified Elasticsearch query (option **Query**).

The include filter also determines the document fields to be inspected by discovery rules. If such a filter has the **Custom** option selected, the rules inspect only the fields specified in the filter's field-value pairs. If the include filter has the **All documents** check box or **Query** option selected, the rules inspect all document fields. The selection of the fields to be inspected is entirely determined by include filters. Exclude filters can exclude documents but not fields from discovery.

---

### **Important**

Within a filter, field-value pairs are combined by AND logic, so the filter matches the documents that match each of the field-value pairs specified. Filters within a unit are combined by OR logic, so the unit includes/excludes the documents matching any one of its filters.

---

To set up a list of field-value pairs, select the **Custom** option. Click in the first column of the list to type the name of the field. To type the value to search for, click in the second column next to the field name. The filter matches documents in which the specified fields have the specified values.

If only a field value is specified, the filter matches documents with that value in any field. The list displays <All> as the name of the field. In this way, you can filter documents by a specific value, regardless of the field in which this value occurs.

If only the name of a field is specified, the filter matches documents with any value in that field. The list displays <All Values> as the value for such a field. In this way, you can specify document fields for discovery by applying discovery rules to data in those fields.

If both the field name and value are specified, then, when executing the discovery task, the field-value pair will be converted to a search query string and passed to Elasticsearch. Only documents returned by that query will match the filter. The value specified for the field must have syntax supported in Elasticsearch query strings.

It is also possible to specify a search query explicitly. To do this, select the **Query** option, and then enter the desired query string in compliance with Elasticsearch syntax (see a query string syntax description at [www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-](http://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl-query-string-)

[query.html#query-string-syntax](#)). In this way, the discovery scope can be determined by using Elasticsearch queries. For example, the query string `author:"John Smith" AND title:(quick OR brown)` generates a search query for documents in which the author field contains John Smith and the title field contains quick or brown.

## Rules and Actions

By using content detection rules, you can define the type of content to discover and specify the actions to perform on the discovered data. Similar to DeviceLock Service's content-aware rules, content detection rules use content groups to determine the data to which a given rule should be applied.

Content detection rules are created based on content groups that enable you to centrally define the types of content to discover. Each rule employs a certain content group, and specifies the actions to apply to the discovered data. The rule's content group specifies the search criteria for the data to which those actions are to be applied.

All content groups are stored in the Content Database. The Content Database for DeviceLock Discovery is stored in the SQL database of the Discovery Server. As a result, all consoles communicating with the Server will operate with a single common Content Database.

---

### Note

Groups stored in the Content Database of the DeviceLock Service can be imported to the DeviceLock Discovery Server. For instructions, see [Importing and Exporting Rules](#).

---

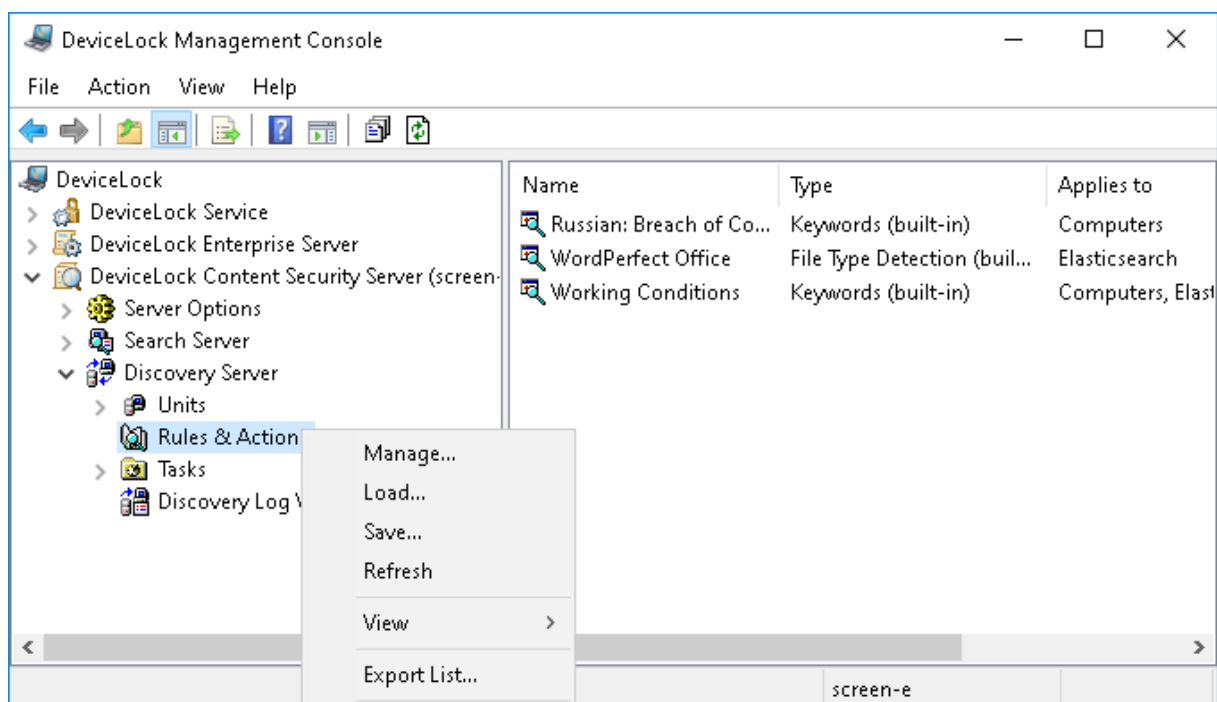
The following content group types are available:

- **File Type Detection** - Identify files by using file type-specific signatures.
- **Keywords** - Look for specific keywords or phrases in data/files.
- **Pattern** - Look for specific text fragments by using Perl regular expressions.
- **Document Properties** - Look for specific document properties, such as size, name, etc.
- **Digital Fingerprints** - Check digital fingerprints of data/files.
- **Complex** - Compose a logical expression of multiple group types.

For more information about content groups, refer to the [Configuring Content Groups](#) section.

## Rules & Actions Node

When you select **DeviceLock Content Security Server > Discovery Server > Rules & Actions** in the console tree, the details pane lists all the content detection rules that currently exist on the server.



In the details pane, the following information is displayed on each rule:

- **Name** - The name that identifies the rule. By default, the rule has the same name as its content group.
- **Type** - The type of the content analysis. Possible values:
  - **File Type Detection** - Recognition and identification of files is based on their characteristic signatures.
  - **Keywords** - Recognition and identification of data/files is based on the specified keywords or phrases.
  - **Pattern** - Recognition and identification of data/files is based on the specified patterns of text described by Perl regular expressions.
  - **Document Properties** - Recognition and identification of files is based on their properties.
  - **Digital Fingerprints** - Recognition and identification of data/files is based on their digital fingerprints.
  - **Complex** - Recognition and identification of data/files is based on the specified content described by a Boolean expression.
- **Applies to** - The unit types for which this rule can be used in discovery tasks. This can be any combination of the following values:
  - **Computers** - The rule can be used to discover files on computers or servers.
  - **Elasticsearch nodes** - The rule can be used to discover documents in Elasticsearch.
- **Action(s)** - The action of the rule. Possible actions:
  - **Delete** - Deleting the detected content.
  - **Safe Delete** - Deleting the detected content with the use of a secure erase procedure as defined in US DoD 5220.22-M.

- **Encrypt** - Encrypting the detected content by using Windows EFS (Encrypted File System).
- **Set permissions** - Setting certain file system permissions on the detected files.
- **Apply to Containers** - Means that the action can be applied to archive files, such as ZIP or RAR files, that hold the detected content.
- **Log** - Recording an event to the Discovery Tasks Log that informs about the detected content.
- **Send Alert** - Sending an alert that informs about the detected content.
- **Notify User** - Notifying the computer user about the detected content.

The shortcut menu on the **Rules & Actions** node includes the following commands:

- **Manage** - Opens a dialog box where you can create, view, modify or delete content detection rules and content groups.
- **Load** - Loads rules from an export file. You can use this command to import content detection rules of Discovery Server as well as content-aware rules and content groups exported from DeviceLock Service.
- **Save** - Saves all rules to an export file.  
You can export rules to a file and then load them from the export file. This function may be useful, for example, when you need to copy rules to another server.
- **Refresh** - Updates the list in the details pane with the latest information.  
Since the console does not automatically update information displayed in the details pane, you need to update the list by using the **Refresh** command.

The shortcut menu on a rule in the details pane includes the following commands:


- **Manage** - Opens a dialog box where you can create, view, modify or delete content detection rules and content groups.
- **Edit Rule** - Opens a dialog box where you can view or change the action of the rule. You can also change the name of the rule.
- **Duplicate Rule** - Creates a new rule with the settings copied from the selected rule. You can change the action and the name of the new rule in the dialog box displayed by this command. By default, the new rule name is composed of the **Copy of** prefix followed by the name of the selected rule. When you create two or more copies of a rule, the new unit name includes a numeric suffix indicating the number of the copy.
- **Delete Rule** - Deletes the selected rule.
- **Refresh** - Updates the list in the details pane with the latest information.  
Since the console does not automatically update information displayed in the details pane, you need to update the list by using the **Refresh** command.

## Defining and Editing Rules and Actions

Content detection rules are defined and edited by using the **Rules & Actions** dialog box.

### *To define a content detection rule*

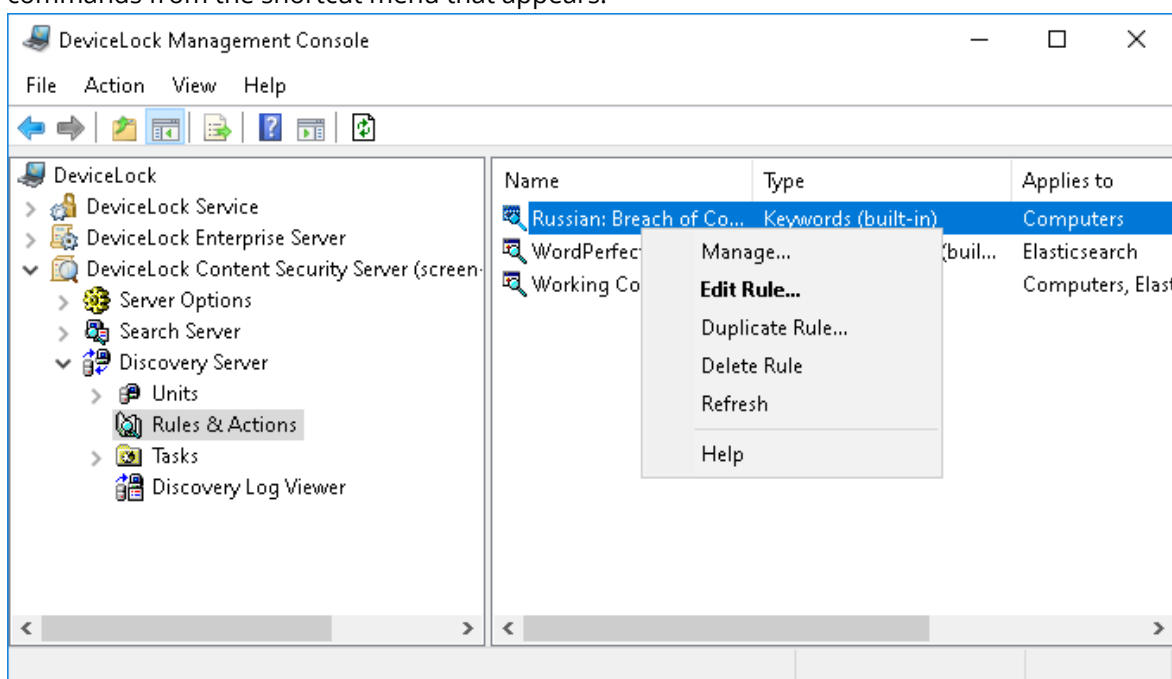
1. Open the DeviceLock Management Console.
2. In the console tree, expand **DeviceLock Content Security Server > Discovery Server**.

3. Under **Discovery Server**, do one of the following:
  - Right-click **Rules & Actions**, and then click **Manage**.
  - OR -
  - Select **Rules & Actions**, and then click **Manage**  on the toolbar.

Configuring content detection rules in DeviceLock Discovery is similar to configuring content-aware rules in ContentLock. For details, refer to the [Content-Aware Rules \(Regular Profile\)](#) section.

### ***To edit, duplicate or delete a content detection rule***

1. Open the DeviceLock Management Console.
2. In the console tree, expand **DeviceLock Content Security Server > Discovery Server**.
3. Under **Discovery Server**, select **Rules & Actions**.
4. In the details pane, right-click the rule you want to edit, duplicate or delete, and then use the commands from the shortcut menu that appears:



## Using the “Rules & Actions” dialog box

You can define and edit content detection rules by using the **Rules & Actions** dialog box. Right-click **Rules & Actions** in the console tree, and then click **Manage** to open that dialog box. The **Rules & Actions** dialog box provides the tools for managing content groups and content discovery rules for Discovery Server.

Content detection rules are created based on content groups that enable you to centrally define the types of content to discover. You can use the built-in content groups as they are, create their editable copies (duplicates) or create your own content groups to suit your particular organization’s needs.

### ***To view a content group***

- In the upper pane of the dialog box, under **Content Database**, select a content group, and then click **View Group**.

You cannot edit built-in content groups but you can create and edit their copies to suit the needs of your organization.

#### ***To copy a content group***

1. In the upper pane of the dialog box, under **Content Database**, select a content group, and then click **Duplicate**.
2. In the dialog box that appears, edit the content group as required, and then click **OK**. The content group you created is added to the list of content groups under **Content Database** in the upper pane of the **Rules & Actions** dialog box.

You can modify or delete custom content groups at any time.

#### ***To modify or delete a custom content group***

1. In the upper pane of the dialog box, under **Content Database**, select a custom group.
2. To modify the selected group, click **Edit Group**. In the dialog box that appears, make the necessary changes, and then click **OK**.

- OR -

To delete the selected group, click **Delete Group** or press the DELETE key.

3. In the **Rules & Actions** dialog box, click **OK** or **Apply** to save the changes.

You can test any built-in or custom content group to see whether specified files match with it. By using these tests, you can verify that the rules that are created based on the content groups meet your specific business requirements.

#### ***To test a content group***

1. In the upper pane of the dialog box, under **Content Database**, select a content group, and then click **Test Group**. You can test only one group at a time.
2. In the dialog box that appears, locate and open the file to use for testing the selected content group.

The console displays the **Result** message box. If the file matches the content group, the message box contains the following text: "Selected file matches with the group." If the file does not match the content group, the message box contains the following text: "Selected file does not match with the group."

---

#### **Note**

When testing is in progress, the console stops responding (hangs).

---

Content detection rules are created based on either the built-in or custom content groups.

#### ***To define a content detection rule***

1. In the upper pane of the dialog box, under **Content Database**, select the desired content group, and then click **Add**.



---

**Note**

For each rule, you can choose only one content group.

---

2. In the **Add Rule** dialog box that appears, specify the rule properties, and then click **OK**.  
The rule you created is displayed under **Rules & Actions** in the lower pane of the **Rules & Actions** dialog box.
3. Click **OK** or **Apply** to save the rule.

You can modify rule properties such as **Name** and **Actions**.

***To modify rule properties***

1. In the lower pane of the dialog box, under **Rules & Actions**, select a rule, and then click **Edit**.  
- OR -  
Right-click a rule, and then click **Edit**.
2. In the **Edit Rule** dialog box that appears, modify the rule properties as required to meet your needs.
3. Click **OK** to save the changes.

You can export all your current content detection rules to a .dra file that you can import and use on another computer. You can also import content detection rules from a .dra file, as well as import DeviceLock Service's content-aware rules from a .cwl file. Exporting and importing can also be used as a form of backup.

***To export content detection rules***

1. In the lower pane of the dialog box, under **Rules & Actions**, click **Save**.
2. In the dialog box that appears, specify the export file. When you export rules, they are saved in a file with a .dra extension.

***To import content detection rules or content-aware rules***

1. In the lower pane of the dialog box, under **Rules & Actions**, click **Load**.
2. In the dialog box that appears, locate and open the file containing the earlier-exported rules.  
You can import only one .dra or .cwl file at a time.

You can delete content detection rules when they are no longer required.

***To delete a content detection rule***

- In the lower pane of the dialog box, under **Rules & Actions**, select the rule and then click **Delete** or right-click the rule, and then click **Delete**.

## Using the "Edit Rule" dialog box

When having detected any content that matches a given rule, DeviceLock performs the action specified by that rule. Use the **Edit Rule** dialog box to view or change the action of a particular rule:

1. Open the DeviceLock Management Console, and then, in the console tree, select **DeviceLock Content Security Server > Discovery Server > Rules & Actions**.
2. In the details pane, right-click the rule, and then click **Edit Rule** on the shortcut menu to open the **Edit Rule** dialog box:

3. Use the following settings provided in the **Edit Rule** dialog box:
  - **Name** - View or change the name of the rule.  
By default, the rule has the same name as its content group. The name of the rule can be changed if needed.  
To view this rule's content group, click the **View Group** button in the bottom left corner of the dialog box. The console displays the properties of the group in a separate dialog box, allowing property values to be viewed but not modified.
  - **Applies to** - Choose the unit type/s for which this rule can be used in discovery tasks:
    - **Computers** - The rule can be used to discover files on computers or servers.
    - **Elasticsearch nodes** - The rule can be used to discover documents in Elasticsearch.

---

#### Note

Rules that apply to Elasticsearch nodes can only log events and send alerts. Other actions are not available in this case.

---

- **Take No Action** - Select to leave the detected content intact. This option should be used when configuring the rule to log a discovery event, alert or notify about the discovery.
- **Delete** - Select to delete the detected content. The following option is available:

- **Safe Delete** - Deletes the detected content using a secure erase procedure as defined in US DoD 5220.22-M.
- **Encrypt** - Select to encrypt the detected content using Windows EFS (Encrypted File System). To enable this action, you have to configure file encryption as follows:
  - a. Select the **Encrypt** option, and then click the **Details** button.
  - b. In the **Encryption Details** dialog box that appears, click **Add**.
  - c. In the dialog box that appears, select a certificate from the list of available encryption certificates.

---

#### Note

The list of available encryption certificates corresponds to the list of Personal Certificates of the user under whose account the management console is launched. You can view Personal Certificates in the **Certificates** console. For details, see Microsoft's article at [technet.microsoft.com/library/cc512680.aspx](https://technet.microsoft.com/library/cc512680.aspx).

During the encryption, a Recovery Agent EFS certificate is added.

---

Encryption does not function when using a remote file system in agentless scanning or when SMB resource scanning is performed. This limitation is specific to EFS and not to DeviceLock Discovery.

---

#### Note

If a file matches multiple rules with the **Encrypt** action, it will be encrypted with all certificates specified in all matching rules.

---

- **Set Permissions** - Select to set file access permissions on the detected content. Click the **Set Permissions** button to open the standard file permissions dialog provided by the operating system.

---

#### Note

If a file matches multiple rules with the **Set Permissions** action, the resulting permission settings on the file will be determined by joining all access control lists (ACL) from all matching rules.

---

Permission conflict resolving: If a file matches multiple rules that specify mutually exclusive permissions, the resulting ACL on that file will be configured by setting individual access parameters. For example, suppose a given file matches two rules, one of which specifies Allow Full Control while the other one specifies Deny Write for the same user. In this case, the resulting ACL will be as follows: Allow Read, Read & Execute; Deny: Write.

If the different rules specify different users or user groups, any access control rights specified by these rules are joined together, and the resulting ACL is determined by Windows.

- **Can Apply Actions to File Containers (Archives)** - Select to allow applying an action (**Delete**, **Set Permissions**, **Encrypt**) to the entire compressed archive (such as a ZIP or RAR file) in which the matching content was discovered. If this option is not selected, the action will not be applied to the container.

---

**Note**

This option also affects saved emails (EML), Adobe Portable Document Format (PDF) files, Rich Text Format (RTF), AutoCAD files (.dwg, .dxf), and Microsoft Office documents (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx).

---

- **Log** - Select to have the rule record a discovery event to the tasks Log (see [Tasks Log Viewer](#)).
  - **Send Alert** - Select to have the rule alert the administrator about the detected content.
  - **Notify User** - Select to have the rule notify the user with a message displayed in the system tray.
- 

**Note**

User notification is not available in Agentless mode.

---

## Importing and Exporting Rules

You can export all your current Discovery Rules and Actions to a .dra file that you can import and use on another computer. You can also import Discovery Rules and Actions from a .dra file, as well as import content-dependent detection rules from a Content-Aware Rules .cwl file. Exporting and importing can also be used as a form of backup.

You can export Discovery Rules and Actions by using the **Save** button in the **Rules & Actions** dialog box. The **Load** button in that dialog box imports Discovery Rules and Actions from either a .dra or .cwl file.

Another option is to use the **Save** and **Load** commands on the **Rules & Actions** node in the DeviceLock Management Console.




### ***To export Discovery Rules and Actions***

1. In the console tree, expand **DeviceLock Content Security Server > Discovery Server > Rules & Actions**, right-click the **Rules & Actions** node, and then click **Save**.
2. In the **Save As** dialog box that appears, specify the export file to hold the exported rules.  
*When you export rules, they are saved in a file with the .dra file name extension.*

### ***To import Discovery Rules and Actions***

1. In the console tree, expand **DeviceLock Content Security Server > Discovery Server > Rules & Actions**, right-click the **Rules & Actions** node, and then click **Load**.
2. In the **Open** dialog box that appears, select the .dra or .cwl file that holds the exported rules.  
*You can import only one .dra or .cwl file at a time.*

Content-dependent detection rules in .cwl format can be loaded from a file. When loading rules from a .cwl file, **Log Event** and **Send Alert** parameters are automatically converted into **Log** and **Send Alert** respectively. If the source rule does not have these parameters, you will need to specify the required action. Such rules will be displayed with an exclamation point icon as shown in the screen below.

Rules & Actions		
Name	Type	Action(s)
 Acquisition	Keywords (built-in)	Delete (Apply To Containers), Send Alert
 Confidential	Keywords (built-in)	
 Executable	File Type Detection (built-in)	Log, Notify User

## Important

It is not possible to use a list of imported rules in which there is a rule marked with an exclamation point. Such rules must be re-configured by hand in order to assign an action or set up logging, alerting, or notification. Once all rules are correctly configured, the list is ready to use.

## Tasks

In DeviceLock Discovery, all actions (computers scanning, content checking and applying actions to discovered content) are performed by tasks.

A single DeviceLock Discovery license can support an unlimited number of tasks. The maximum number of tasks is only limited by available memory, CPU and network's bandwidth capacity. Please keep in mind that the server should have sufficient resources to communicate with at least 10 remote computers simultaneously.

DeviceLock Discovery Server imposes the following limits on concurrent communications:

- For scanning with DeviceLock Discovery Agent:
  - The Server sends tasks to remote agents in up to 5 threads. This number cannot be changed.
  - The Server collects scanning logs and status updates from remote agents in up to 10 threads. This value can be changed by modifying the following registry value:
    - Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockContentSecurityServer\DiscoverySettings
    - Value: MaxConcurrentAgents=dword:<number\_of\_threads>  
In this value, <number\_of\_threads> must be an integer between 1 and 64.
- For agentless scanning:
  - The Server scans remote computers in up to 10 threads. This value can be changed by modifying the following registry value:
    - Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockContentSecurityServer\DiscoverySettings
    - Value: MaxConcurrentLocalAgents=dword:<number\_of\_threads>  
In this value, <number\_of\_threads> must be an integer between 1 and 64.

The following activities occur during task execution:

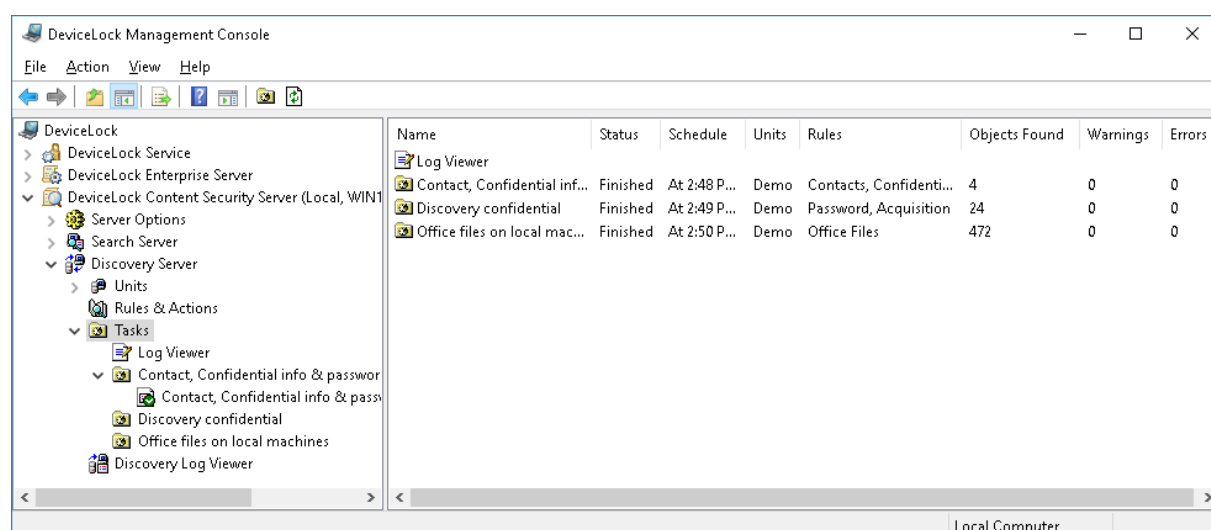
1. Write status information to the tasks Log ( [Tasks Log Viewer](#)), including data about computers being scanned with DeviceLock Discovery.
2. Perform actions on discovered content (as defined in the Rules & Actions).
3. Create a report containing all relevant information about the task execution.

The tasks are controlled with the management console as described below.

Action	Description
View Log	<p>To view Discovery tasks log:</p> <ol style="list-style-type: none"> <li>1. In the management console tree, expand <b>DeviceLock Content Security Server &gt; Discovery Server &gt; Tasks</b>.</li> <li>2. Under the <b>Tasks</b> node, click <b>Log Viewer</b>.</li> </ol> <p>The log view will appear in the details pane. The log view is common to all tasks.</p>
Edit Task	<p>To view or change task parameters:</p> <ol style="list-style-type: none"> <li>1. In the management console tree, expand <b>DeviceLock Content Security Server &gt; Discovery Server &gt; Tasks</b>.</li> <li>2. Under the <b>Tasks</b> node, right-click the task, and then click <b>Edit Task</b> on the shortcut menu.</li> </ol> <p>You can view or change the task parameters in the wizard that appears.</p>
View Report	<p>To view the report of a certain task:</p> <ol style="list-style-type: none"> <li>1. In the management console tree, expand <b>DeviceLock Content Security Server &gt; Discovery Server &gt; Tasks</b>.</li> <li>2. Under the <b>Tasks</b> node, expand the task whose report you want to view.</li> <li>3. Click the report under the task node in the console tree.</li> </ol> <p>The report view appears in the details pane. Reports are task-specific; in order to view reports produced by multiple tasks, you will have to expand each task and view each task's corresponding report.</p>

## Tasks Node

All discovery tasks along with their log and reports are available in the console tree under **DeviceLock Content Security Server > Discovery Server > Tasks**.



Select the **Tasks** node in the console tree to view a list of discovery tasks. The list in the details pane displays the following information on each task:

- **Name** - The name of the task.
- **Status** - One of the following:
  - **Canceled** - The task was launched and manually canceled via the task's shortcut menu. No report is created for canceled tasks.
  - **Expired** - The task was launched but never reported back, and was discarded after the expiration of [Keep-alive timeout](#) for one or more computers specified in the task. The **Expired** status is also assigned for tasks terminated after the time specified in [Stop task if runs longer than](#) has expired.  
If the task is expired, reports are created based on all information received from the agents prior to expiration.
  - **Failed** - The task failed to execute on all computers scheduled to be scanned by the task (for example, if all computers were unavailable).  
The report will be created containing the **Failed to scan** table listing the computers that failed to scan and including the failure reason.
  - **No License** - The task was launched, but the installed license was insufficient to scan at least one resource. The report will be created.
  - **Finished** - The task has successfully completed and will not be recurred. The report will be created.
  - **Running** - The task is running.
  - **Waiting** - The task was not and will not be launched (e.g. the **Active** flag is not set).
  - **Scheduled** - The task is scheduled to run in the future. This status does not specify whether or not the task was ever executed in the past.
- **Schedule** - Identifies the task schedule.
- **Units** - Lists the units specified in the task.
- **Rules** - Lists the rules specified in the task.
- **Objects Found** - The number of objects discovered by the task.
- **Warnings** - The number of warnings issued by the task.
- **Errors** - The number of scanning errors the task encountered.

The shortcut menu on the **Tasks** node includes the following commands:

- **Create Task** - Creates a new task. You can specify the desired task settings in the dialog boxes that appear when you select this command.
- **Refresh** - Updates the list of tasks with the latest information.

The shortcut menu on a task in the details pane includes the following commands:

- **Edit Task** - Opens the dialog boxes where you can view or change the settings of the selected task.
- **Duplicate Task** - Creates a new task with the settings copied from the selected task. You can view or change the settings of the new task in the dialog boxes displayed by this command.

By default, the new task name is composed of the **Copy of** prefix followed by the name of the selected task. When you create two or more copies of a task, the new task name includes a numeric suffix indicating the number of the copy.

- **Delete Task** - Deletes the selected task.  
If a given task was ever run, and thus has any reports, then the console prevents deletion of that task. To delete such a task, you first need to delete the task's reports.
- **Run Task** - Causes immediate execution of the selected task. You can run any task except of those already running.
- **Stop Task** - Causes immediate stop of the selected task. This command replaces the **Run Task** command for the tasks that are currently running.
- **Generate New Report** - Initiate report generation. Depending on the context, this command can be used as follows:
  - During task execution - If the task is currently running and has some progress, report generation is not possible.
  - After task finished - You can re-create reports in some time after the task finished. This can be used to produce the complete report if some tasks finished after the [Keep-alive timeout](#) has expired. In this case, agents that took longer than that to finish their jobs will report back to the server; the server will collect logs from these agents, but the report will not re-generate automatically. By using **Generate New Report**, you will produce the most complete report using all available information.
- **Refresh** - Updates the list of tasks with the latest information.

## Creating a Task

Tasks are created with a wizard. To create a task, do the following:

1. Open the task creation wizard:
  - In the DeviceLock Management Console, expand **DeviceLock Content Security Server > Discovery Server > Tasks**, right-click **Tasks**, and then click **Create Task** on the shortcut menu.
2. In the **Select Units** dialog box that appears, select the units that will be scanned by the task:
  - Select one or more units in the **Available Units** list, and then click **Add**. To select multiple units, click while holding down the Shift or Ctrl key. The units you have added appear in the **Selected Units** list.

For each unit, the list indicates the unit's name and type. The name serves to identify the unit. The type identifies the unit's intended purpose: scan computers (**Computers** unit type) or scan Elasticsearch nodes (**Elasticsearch nodes** unit type). For the **Computers** unit type, in brackets it is indicated what kind of computer list the given unit has: [Static list](#) or [Dynamic list](#).

To review the settings of the selected unit, click the **View** button. In the dialog box that appears, you can view but not change the unit's settings.
3. Click **Next** to continue.
4. In the **Select Rules & Actions** dialog box that appears, select the rules that will be applied by the task:



- Select one or more rules in the **Available Rules & Actions** list, and then click **Add**. To select multiple rules, click while holding down the Shift or Ctrl key. The rules you have added will appear in the **Selected Rules & Actions** list.

For each rule, the list provides the following rule information:

- **Rule Name** - The name that identifies the rule.
- **Rule Type** - The type of the content group used by this rule for content discovery.
- **Applies To** - The unit types for which this rule can be used.
- **Action(s)** - The identifiers of the actions this rule performs during content discovery.

The list of available rules is limited to the rules that apply to the type of the units selected for this task. For example, when only Elasticsearch units are selected, the list contains the rules that apply to Elasticsearch nodes only or to Computers and Elasticsearch nodes, and does not contain the rules that apply to Computers only. When units of all types are selected, the list contains all existing rules.

To review the settings of the selected rule, click the **View** button. In the dialog box that appears, you can view but not change the rule's settings.

5. Click **Next** to continue.
6. In the **Set Task Schedule & Advanced Settings** dialog box that appears, you can change the name of the task, configure the task to run on a scheduled basis, and specify additional settings that affect execution of the task:
  - **Task Name** - Identifies the name of the task. The task will appear under that name in the management console.
  - **Active** - Select this check box to activate the task according to the schedule, or clear to deactivate it.  
If the **Active** check box is not selected, the task will not be executed by the schedule.
  - **Schedule** - To configure a schedule for the task, use the following options:
    - **One Time** - The task will be launched once on the time and date specified. Choose the date and time to run the task, or select the **Now** check box to run the task right after it has been created or modified.

---

#### Note

If you specify a date/time in the past, the following message is displayed when you click **Next**:  
"The specified date is earlier than the current date."

---

- **Hourly** - The task will be executed on an hourly basis. The task will recur after the specified number of hours. You will be able to specify the number of hours to pass between scheduled scanning attempts.
- **Daily** - The task will be executed on a daily basis. The task will recur after the specified number of days. You will be able to specify the number of days to pass between scheduled scanning attempts.
- **Weekly** - The task will be executed on a weekly basis. The task will recur after the specified number of weeks. You will be able to specify the number of weeks to pass between scheduled scanning attempts, and set days of weeks on which the scanning task will be executed.

- **Monthly** - The task will be executed every month on a specified day. You will be able to specify calendar months on which the task will be executed. You will be also able to specify calendar days of month or days of week on which the scanning task will be executed.

#### Note

If you configure a recurrent task, the task will run periodically according to a set schedule. If, however, a task execution does not finish before a next run of the task upon schedule, the next run of that task is delayed until the preceding execution of the task has finished.

- **Advanced Settings** - Use these settings to control the task's behavior during execution:
  - **Stop task if runs longer than** - Specifies that the task will be force stopped if it takes longer than a specified period of time to complete.

This setting is used to ensure successful automated operation even if the rules are too complex or the scanned data set too big to complete on a timely basis.

- **Scan priority** - Specifies process priority and sets the amount of simultaneous scanning threads depending on the number of available processors and/or processor cores.

- The **Below Normal** or **Low** setting will only use one processor/core for scanning and set the “Below Normal” or “Low” process priority, respectively.
- The **Above Normal** or **Normal** setting will use one half of all available processors/cores and set the “Above Normal” or “Normal” process priority, respectively.
- The **High** setting will use all available processors/cores except one, and set the “High” process priority.
- The **Realtime** setting will devote all available processors/cores to the scanning task, and set “Realtime” priority to the process.
- **Number of retries** - The number of times that will be performed if the scanning attempt returns status indicating an error. The value of 0 means that no retries will be performed if the first attempt fails.
- **Retry timeout** - Specifies how many seconds DeviceLock waits before attempting to perform the next scanning attempt in the case the previous attempt failed.

- **Keep-alive timeout** - Specifies the number of hours the server will wait for each agent to collect scanning logs. If no logs were collected after the timeout has passed, the server will stop waiting for that agent.

Keep-alive timeout:  hour(s)

If the agent reports later on and after the timeout has passed, the logs will be collected and processed as usual.

7. Click **Next**. The confirmation dialog will appear listing parameters of the newly created task. Click **Finish** to complete the wizard. The newly created task will be saved and scheduled.

You can edit, delete, duplicate or run tasks, refresh task list or generate a new report by using the task's shortcut menu. For description of the menu, see [Tasks Node](#) earlier in this document.

## Task and Its Reports

The console displays discovery tasks in the console tree under **DeviceLock Content Security Server > Discovery Server > Tasks**.

The shortcut menu on a discovery task in the console tree includes the same commands as the task's shortcut menu in the details pane (for description of commands, see [Tasks Node](#) earlier in this document).

When you select a discovery task in the console tree, the details pane lists the reports produced by that task. The list in the details pane displays the following information on each report:

- **Name** - Report name. By default, includes the task name followed by the date and time of the task run.
- **Type** - One of the following:
  - **Scheduled** - Report generated automatically upon task completion.
  - **Manual** - Report generated by hand, using the **Generate New Report** command.
- **Status** - One of the following:
  - **Generating** - Report creation is in progress.
  - **Ready** - Report created successfully.
  - **Error** - Report encountered an error.
- **Objects Found** - The number of objects discovered by the task.
- **Warnings** - The number of warnings issued by the task.
- **Errors** - The number of scanning errors the task encountered.
- **Started** - Date and time that the report creation started.
- **Finished** - Date and time that the report creation was completed.
- **Scheduled by** - Identifies the user account that started the task (in case of report type of **Scheduled**) or generated the report (in case of report type of **Manual**).
- **Scheduled from** - Identifies the computer from which the task was started (in case of report type of **Scheduled**) or the report was generated (in case of report type of **Manual**).

The shortcut menu on a report in the details pane includes the following commands:

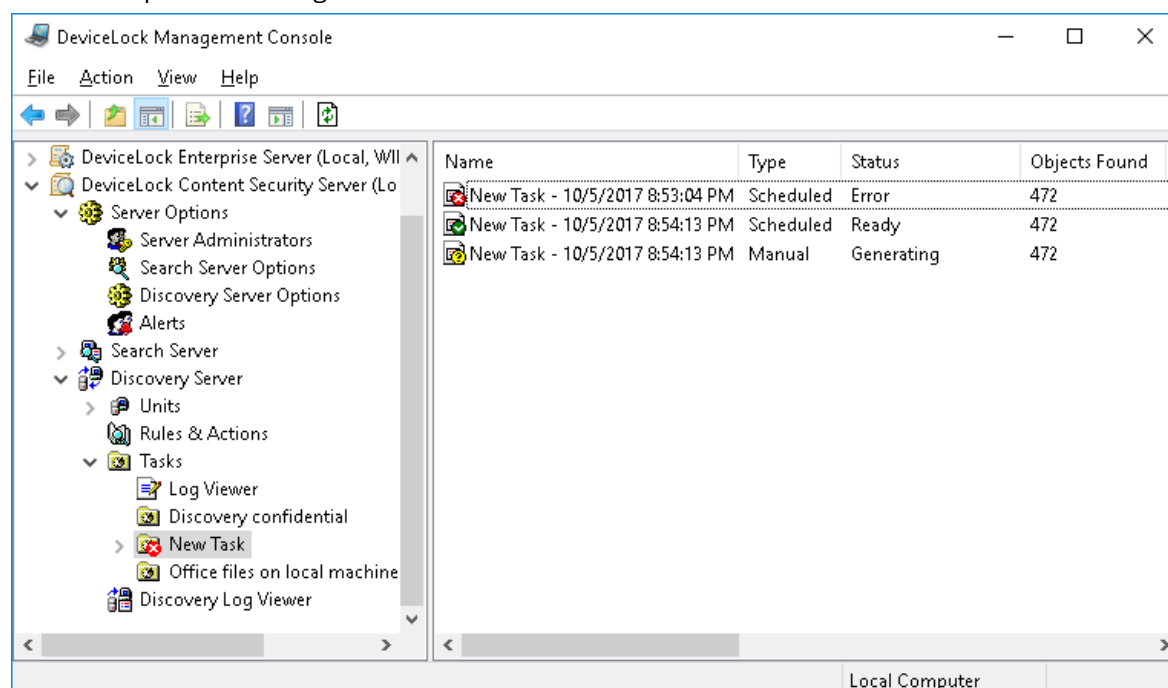
- **Open** - Displays the report in the details pane. This command is available for reports with the status of **Ready** (green icon).  
Another way to open a task's report is by selecting the report under the node representing that task in the console tree.
- **Show error** - Displays error information about the report. This command is available for reports with the status of **Error** (red icon).
- **Rename** - Changes the name of the selected report. You can specify a new name in the dialog box displayed by this command.
- **Delete Report** - Deletes the selected report.  
You can delete multiple reports at a time: Click while holding down Shift or Ctrl to select reports, right-click the selection, and then click **Delete Reports**.
- **Generate New Report** - Appears on the menu when you select multiple reports. Generates a single aggregated report by using information available in all selected reports.
- **Refresh** - Updates the list of reports with the latest information.

## Viewing the report list

Each task produces reports detailing the scanning results in a human-readable form. To access reports, do the following:

1. Open the DeviceLock Management Console.
2. In the console tree, expand **DeviceLock Content Security Server > Discovery Server > Tasks**.
3. Under the **Tasks** node, select and expand the node that represents the task whose report you want to access.

The list of the given task's reports appears in under the task node in the console tree as well as in the details pane on the right of the console tree:



The following types of report are available:

- **Scheduled** - Reports automatically generated after the task finishes.
- **Manual** - Reports manually generated by the user via the **Generate New Report** command.

The icon in the first column represents report status. The following statuses are available:

- **Generating** - A yellow icon. The report is being generated. Wait for the generation to finish before opening the report.
- **Ready** - A green icon. Double-click on the report to open.
- **Error** - A red icon. Double-click on the report to view details about the error.

For more information, see description of the report list in the [Task and Its Reports](#) section.

To manage reports, select one or more reports in the details pane, right-click the selection, and use the commands from the shortcut menu. Description of commands can be found in the [Task and Its Reports](#) section earlier in this document.

---

**Note**

To select multiple reports, click while holding down the Shift or Ctrl key.

---

## Viewing a Report

When you expand the node representing a discovery task in the console tree, and select a report under that node, the details pane displays report pages. Another way to view a report is by using the **Open** command on the shortcut menu or by double-clicking the report list item in the details pane.

The shortcut menu on a report in the console tree includes the following commands:

- **Open** - Displays the report in the details pane.
- **Rename** - Changes the name of the report. You can specify a new name in the dialog box that appears.
- **Delete Report** - Deletes the selected report.
- **Refresh** - Updates the report in the details pane.

DeviceLock Discovery Server generates multi-page reports in HTML format.

---

**Note**

If JavaScript is not enabled in your Web browser, the following error appears when viewing a report: "For full functionality of this page it is necessary to enable JavaScript. See your web browser manual or help on how to enable JavaScript."

To view reports, enable JavaScript in your Web browser. For instructions, see the "How to enable JavaScript in your browser" guide at <http://www.enable-javascript.com>.

---

Discovery Server allows automatic or manual generation of reports using data returned by scanning agents. Use reports to arrange and display information about discoveries and actions performed by the scanning agents.

Reports are created automatically by the tasks. You can also generate reports manually by using DeviceLock Management Console.

The report contains detailed information about the results of the scan.

The first page of the report may contain the following information:

- **Header** - Displays the name of the report, and contains information about when the scan started and finished, the name of the user who requested the report, and the name of the computer from which the report was initiated.
- **Discovery results** - Contains a summary of discovery results and actions performed on the discovered content. If the discovery task did not make any discoveries, this section displays **Discovery results: None**.

Information in this section includes:

- **Object Name** - Lists the rules along with the units in which the rule made a discovery.

In the list of rules and units, the report displays the following information:

- **Log** - Indicates how many discovery events have been logged.
- **Alert** - Indicates how many administrator alert about the discovery have been sent.
- **Notify** - Indicates how many user notifications about the discovery have been displayed.
- **Delete** - Indicates the number of occurrences where detected content has been deleted.
- **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.
- **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.
- **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.
- **Rules** - This section contains descriptions of all rules specified in the task, including those not included into the **Discovery results** table.
- **Failed to scan** - If the discovery task was unable to scan any of its target computers and/or Elasticsearch nodes, the report contains a summary of errors:
  - **Unit/Target** - A list of units with the computers/nodes that failed to scan.
  - **Error message** - A description of the error due to which the computer/node failed to scan.
  - **Date/Time** - The date and time that the error occurred.

---

## Note

Many items in the report are clickable links. Clicking a certain element may open a page with information on the item you clicked), or open the log viewer with a pre-filled filter to display all records relevant to the item you clicked. For example, clicking the number in the **Total** line opens the log viewer that displays all actions calculated in the referring table.

For more information and instructions on how to work with reports, see [Navigating Reports](#).

---

You can click the plus sign **[+]** on the left of each object to expand. To expand all objects, click the plus sign **[+]** on the left of the **Object Name** heading.

Subsequent report pages contain detailed information, including:

- **Header** - Displays the name of the report, and contains information about when the scan started and finished, the name of the user who requested the report, and the name of the computer from which the report was initiated.
- **Discovery results** - Lists the scanned targets (computers and Elasticsearch nodes). The list can be expanded by clicking the name of a target. This will display a list of discovered files.

---

#### Note

You can switch the order in which targets and files are displayed, making file names appear as expandable branches and target names as leaf items. The list display depends on the type of the link you clicked to get to this report.

For more information on the report items display, see [Navigating Reports](#).

---

Information in this section includes:

- **Object Name** - Displays target names and file names, depending on the view mode. Either targets are listed, each of which has an associated list of files discovered on it, or files, each of which has an associated list of targets on which this file was discovered.

In the list of targets and files, the report displays the following information:

- **Log** - Indicates how many discovery events have been logged.
- **Alert** - Indicates how many administrator alert about the discovery have been sent.
- **Notify** - Indicates how many user notifications about the discovery have been displayed.
- **Delete** - Indicates the number of occurrences where detected content has been deleted.
- **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.
- **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.
- **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.

---

#### Note

Some report items can be clicked. Clicking a file name or target name will display the list of associated targets or files, whereas clicking an underlined number will open the **Log Viewer**.

For more information and instructions on how to work with reports, see [Navigating Reports](#).

---

Flat table view is also available that lists either all discovered files or all targets where at least one file with the desired content was discovered. Such a report does not contain nested lists of different levels, but by clicking on a file, you can open a list of targets where this file was discovered, and clicking a target can open a list of files discovered on this target.

In the flat table view, the following information is available:

- **Header** - Displays the name of the report, and contains information about when the scan started and finished, the name of the user who requested the report, and the name of the computer from which the report was initiated.

- **Discovery results** - Lists the files and targets (computers and Elasticsearch nodes) discovered by the combination of units and rules. This list can be displayed in one of the following views depending on the link used to get to the flat table view:
  - **Object Name:**
    - **Targets for** <file name> **for** <unit name> **and** <rule name> - Lists the targets on which a certain file was discovered by a certain rule in a certain unit.  
- OR -
    - **Targets for** <file name> **for** <rule name> - Lists the targets on which a certain file was discovered by a certain rule.  
- OR -
    - **Data for** <target name> **for** <unit name> **and** <rule name> - Lists the files discovered on a certain target by a certain rule for a certain unit.  
- OR -
    - **Data for** <target name> **for** <rule name> - Lists the files discovered on a certain target by a certain rule. If a file has more than one name (has different aliases), the number of aliases is displayed in parenthesis next to the file name.

In all of these views, the file, target, rule, and unit names are specified by the <file name>, <target name>, <rule name>, and <unit name> variables, respectively.

In the list of resources and files, the report displays the following information:

- **Log** - Indicates how many discovery events have been logged.
- **Alert** - Indicates how many administrator alert about the discovery have been sent.
- **Notify** - Indicates how many user notifications about the discovery have been displayed.
- **Delete** - Indicates the number of occurrences where detected content has been deleted.
- **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.
- **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.
- **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.

One more report type is alias view. If the task discovered several files with the same content but different names, these names are referred to as aliases. The alias report lists the aliases of the discovered files. Clicking an alias of a file displays a list of targets on which the file was discovered. You can also display this list by clicking the plus sign **[+]** next to the alias.

The alias view has two tables. The first is the alias table, the second is a list of resources (computers and Elasticsearch nodes) on which the file with a given alias from the first table was discovered. In the alias view, the following information is available:

- **Header** - Displays the name of the report, and contains information about when the scan started and finished, the name of the user who requested the report, and the name of the computer from which the report was initiated. The header also contains information about the report's unit, rule, and target.



- **Aliases** - Lists the aliases (different names of the same file) discovered by the combination of units and rules on a given target. This information includes:
  - **Object Name** - All the names of the discovered file. For each name, the report lists the targets on which the file was found under that name.

In the list of files, the report displays the following information:

- **Log** - Indicates how many discovery events have been logged.
- **Alert** - Indicates how many administrator alert about the discovery have been sent.
- **Notify** - Indicates how many user notifications about the discovery have been displayed.
- **Delete** - Indicates the number of occurrences where detected content has been deleted.
- **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.
- **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.
- **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.
- **Discovery results** - Lists the targets where a given file was discovered under the names specified in the table of aliases. This information includes:
  - **Object name** - All targets containing a particular file are listed under the respective file name.

In the list of targets and files, the report displays the following information:

- **Log** - Indicates how many discovery events have been logged.
- **Alert** - Indicates how many administrator alert about the discovery have been sent.
- **Notify** - Indicates how many user notifications about the discovery have been displayed.
- **Delete** - Indicates the number of occurrences where detected content has been deleted.
- **Encrypt** - Indicates the number of occurrences where detected files have been encrypted.
- **Set Permissions** - Indicates the number of occurrences where file access permissions on detected content have been modified.
- **Warnings** - Indicates the number of file access errors, content analysis errors and errors applying actions to discovered files.

## Navigating Reports

DeviceLock Discovery Server generates dynamic reports with comprehensive navigation structure. These reports enable you to receive detailed information about most items in the report by clicking an item. Most elements in the report are clickable links. Clicking a certain element may transfer you to a different page in the report (opening detailed view for the item you clicked), or open the Log Viewer with pre-filled filter to display all records relevant to the item you clicked.

## Discovery results

The first column of the **Discovery results** table contains a number of clickable items. Clicking a rule or unit displays a shortcut menu.

If you click a rule, the following items are available on the shortcut menu:

- **Targets for Rule** - Displays a list of all targets (computers and Elasticsearch nodes) on which content matching the rule was discovered.
- **Data for Rule** - Displays a list of all files in which content matching the rule was discovered.

If you expand a rule and click one of the units, the following items are available on the shortcut menu:

- **Targets for Unit and Rule** - Displays a list of targets in the selected unit on which content matching the rule was discovered.
- **Data for Unit and Rule** - Displays a list of files from targets in the selected unit in which content matching the rule was discovered.

Certain numbers in the table are clickable. If you hover a mouse over such numbers, they become underlined. Clicking an underlined number in the table opens the **Log Viewer** as described in the [Links to the log viewer](#) section.

## Failed to scan

The report section **Failed to scan** lists all units containing targets (computers and/or Elasticsearch nodes) that failed to scan. Clicking a unit opens a list of targets with the respective error messages. You may encounter the following error messages:

- **Computer is unavailable** - The target computer/server was not available during the scan (for example, turned off or not connected to the network).
- **Installation failed** - The installation of the Discovery agent was not successful on the target computer to scan.
- **Access is denied** - When accessing the target to scan, there was a problem with configured access credentials or certificate.
- **No License** - The number of targets to scan has exceeded the license. You may wish to upgrade your license to scan additional targets.

## Details table

Clicking one of the four menu items described in [Discovery results](#) opens the respective **Details Table**. If you click a target, you are presented with all files discovered by the corresponding rule. If you click a file, you will see all targets on which that file was discovered by the corresponding rule. Which particular list view is displayed is indicated in the **Discovery results** line.

Certain numbers in the table are clickable. If you hover a mouse over such numbers, they become underlined. Clicking an underlined number in the table opens the **Log Viewer** as described in the [Links to the log viewer](#) section.

The number of entries for all tables can be adjusted by changing the following registry values:

- Key: HKEY\_CURRENT\_USER\SOFTWARE\SmartLine Vision\DLManager\Manager
  - Value: DisplayRootCount=dword:<number of root elements>  
The default value is 500.

- Value: DisplayChildCount=word:<number of child elements>  
The default value is 50.

By default, at most 500 root elements (nodes) and 50 sub-nodes of each node will be listed.

## Rules

The **Rules** section lists the rules used in this scan. Clicking a rule name opens the **Rules & Actions** view, with that rule selected in the details pane.

## Links to the log viewer

If you need more details about a certain item in one of the report tables, you may click an underlined item in the header or an underlined number in the table. This will open the log viewer, with the filter options set to ensure that only relevant records are displayed.

The filtering rule is a logical AND of all relevant fields, and is generated as follows:

```
<report ID> AND <column name> AND <rule name> AND <unit name>
```

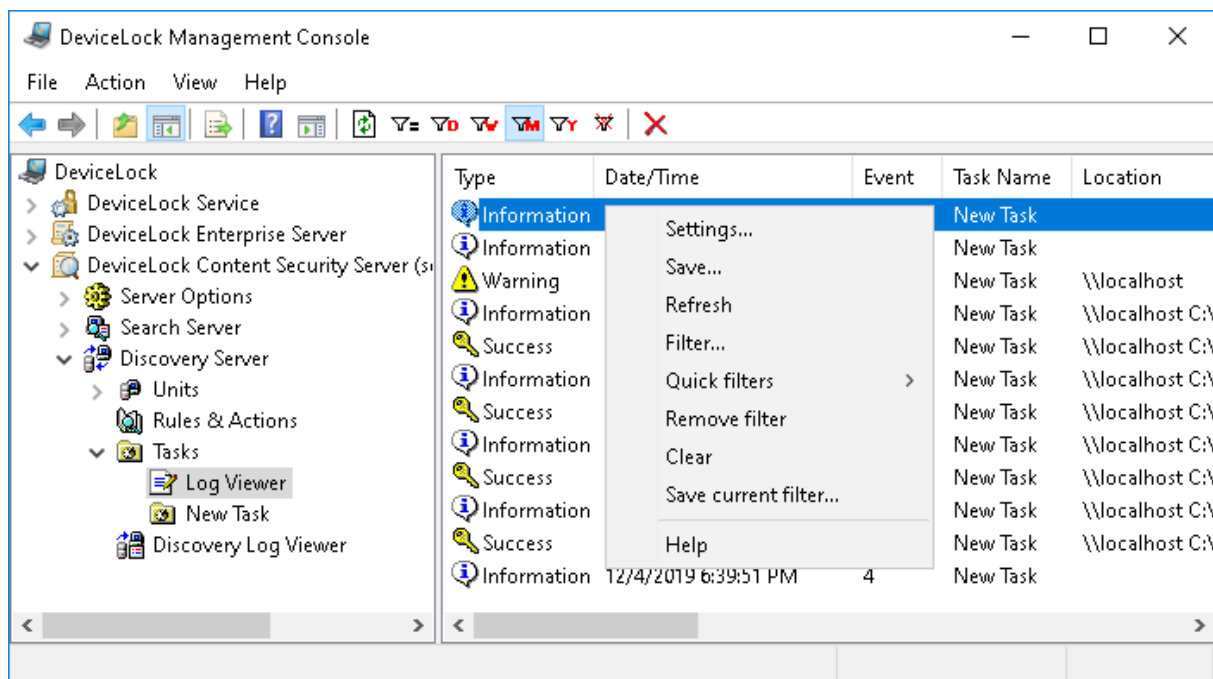
The resulting filter is applied to the log viewer, and you will see only those entries that match the filtering rule. As a result, you will always have the log viewer display information that is relevant to your click. You can reset the filter and view full log results by using the **Reset Filter** command.

## Tasks Log Viewer

This viewer allows you to retrieve the log files produced by discovery tasks. Discovery tasks use this log to write information about scanning activities, discoveries and actions taken to discovered content.

To access the tasks log, do the following:

1. Open the DeviceLock Management Console.
2. In the console tree, expand **DeviceLock Content Security Server > Discovery Server > Tasks**, and then select **Log Viewer** under the **Tasks** node.



The details pane displays a list of events, with the following information on each event:

- **Type** - Event type indicates one of the following:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Date/Time** - Date and time that the event occurred.
- **Event** - ID number of the event.
- **Task Name** - Identifies the discovery task that caused the event.
- **Location** - The name of the resource the event is related to.
- **Actions** - Identifies the action performed by the task on the detected content, such as:
  - **Alert** - Sending an alert that informs about the detected content.
  - **Delete** - Deletion of the detected content.
  - **Delete (Safe Delete)** - Deletion using a secure erase procedure as defined in US DoD 5220.22-M.
  - **Encrypt** - Encrypting the detected content by using Windows EFS (Encrypted File System).
  - **Log** - Recording an event to the Discovery tasks log that informs about the detected content.
  - **Notify** - Notifying the computer user about the detected content.
  - **Set Permissions** - Setting certain file system permissions on the detected files.
- **Name** - The name of discovered file.
- **Reason** - The cause of the event, such as:
  - **Completed** - Completion of the discovery task.
  - **Content-Aware Rule error** - Discovery rule application error.







- **On request** - Discovery task started by hand.
- **On schedule** - Discovery task started by a schedule.
- **Rule** - Discovery rule triggered. The reason specifies the name of the rule followed by a brief description of the content matches, keywords, and/or file types that led to the rule triggering.
- **Information** - Event description that provides details of the actions performed and errors encountered.
- **Unit** - The name of the unit in which the event occurred.
- **Unit Type** - Intended use of the unit in which the event occurred: scan computers (**Computers** unit type) or scan Elasticsearch nodes (**Elasticsearch nodes** unit type).
- **Received Date/Time** - The date and time when the event was received by DeviceLock Discovery Server.

## Managing the Tasks Log

You can manage the log by using commands from the shortcut menu:



- In the console tree, expand **DeviceLock Content Security Server > Discovery Server > Tasks**, and then right-click **Log Viewer** under the **Tasks** node.  
- OR -  
In the console tree, select **DeviceLock Content Security Server > Discovery Server > Tasks > Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings** - View or change the settings that limit the maximum number of event records the log may contain. For instructions, see [To view or change Discovery tasks log settings](#).
- **Save** - Saves the log to the file you specify.
- **Refresh**  - Updates the list of events with the latest information.
- **Filter**  - Displays only the events that match the conditions set. For instructions, see [To configure the Discovery tasks log filter](#).
- **Quick filters** - Choose from the following options to display only records for a certain period of time:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

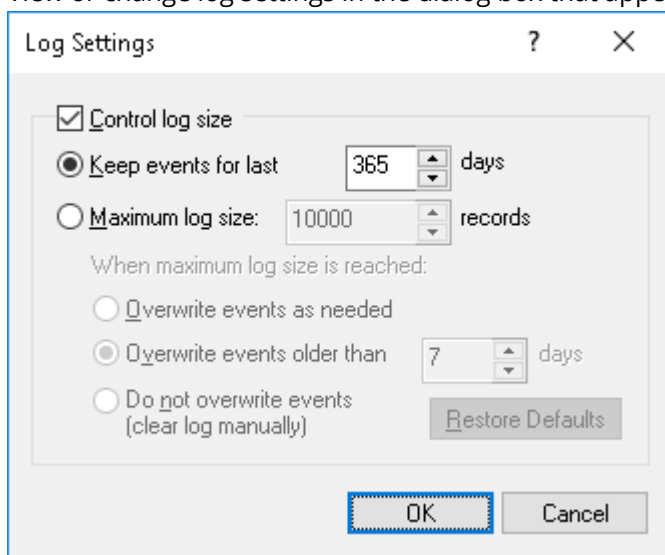
A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Clear**  - Delete all records that currently exist in the log.

This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.

### ***To view or change Discovery tasks log settings***

1. Click **Settings** on the shortcut menu.
2. View or change log settings in the dialog box that appears.



The following log settings are available:

- **Control log size** - Select this check box to allow the server to control the number of records in the log and delete outdated records. If this check box is cleared, the server uses all available database space to store the log.
- **Keep events for last <number> days** - Store records no older than a certain number of days. Then, specify the desired number of days. The default setting is 365 days.
- **Maximum log size: <number> records** - Store no more than a certain number of records. If you select this option, specify the desired number of records, and select the server action to be performed when the log reaches the maximum size:
  - **Overwrite events as needed** - New event records continue to be stored when the maximum log size is reached. Each record of a new event replaces the oldest record in the log.
  - **Overwrite events older than <number> days** - New event records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.
  - **Do not overwrite events (clear log manually)** - New event records are not added when the maximum log size is reached. To enable the server to add new records, the log must be cleared by hand.

---

### **Important**

If the log has no space for new records and log settings do not allow the deletion of old records, then the server does not add any new records to the log.

---

To use the default log size, select the option **Maximum log size** and click **Restore Defaults**. The default log size settings are as follows:

- Maximum log size: 10,000 records
- Overwrite events older than 7 days

### ***To configure the Discovery tasks log filter***

1. Click **Filter** on the shortcut menu.
2. View or change filter settings in the dialog box that appears.

Filter

☒ Include ☐ Exclude

Event types

☒ Success ☒ Warning  
☒ Information ☒ Error

Event ID:

Task name:

Location:

Action:

Name:

Reason:

Information:

Unit:

Generated Date/Time

From:

To:

Received Date/Time

From:

To:

☒ Enable filter

Clear Load Save

OK Cancel

Two filter types are available:

- **Include** - The console displays only the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab.
- **Exclude** - The console does not display the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab.

The filter can be temporarily disabled by clearing the **Enable filter** check box.

---

**Note**

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

When the filter enabled, its conditions are defined by entering values into the following fields:

- **Event types** - Select check boxes to filter events by type:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- String fields that allow you to include or exclude events depending upon whether event data matches the filter string specified. For example, to filter events by the name of the task that caused the event, specify a filter string in the **Task name** field. To filter events with certain IDs, enter ID numbers separated by a semicolon in the **Event ID** field.

The following string fields are available:

- **Event ID** - ID number of the event.
- **Task name** - The name of the task that caused the event.
- **Location** - The name of the resource the event is related to.
- **Action** - The name of the action that caused the event. You can type or select a name from the following list:
  - **Alert** - Means sending an alert that informs about the detected content.
  - **Delete** - Indicates deletion of the detected content.
  - **Delete (Safe Delete)** - Means deletion using a secure erase procedure as defined in US DoD 5220.22-M.
  - **Encrypt** - Indicates encrypting the detected content by using Windows EFS (Encrypted File System).
  - **Log** - Means recording an event to the Discovery tasks log that informs about the detected content.
  - **Notify** - Means notifying the computer user about the detected content.
  - **Set Permissions** - Indicates setting certain file system permissions on the detected files.
- **Name** - The name of the discovered file.
- **Reason** - The reason that triggered the event. You can type or select a reason from the following list:
  - **Completed** - Completion of the discovery task.
  - **Content-Aware Rule error** - Discovery rule application error.
  - **On request** - Discovery task started by hand.
  - **On schedule** - Discovery task started by a schedule.
  - **Rule** - Discovery rule application.



- **Information** - Detailed description of the event that includes details of the actions performed and errors encountered
- **Unit** - The name of the unit in which the event occurred.

---

### Note

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

- **Generated Date/Time** - In this area, the following fields can be used to specify the event range by the date and time that the event occurred:
  - **From** - The beginning of the range of events to filter. Possible values: **First Record** (selected by default) and **Records On**. Select **First Record** to filter events starting from the earliest generated one. Select **Records On** to filter events that occurred no earlier than a specific date and time.
  - **To** - The end of the range of events to filter. Possible values: **Last Record** (selected by default) and **Records On**. Select **Last Record** to filter events up to the latest generated one. Select **Records On** to filter events that occurred no later than a specific date and time.
- **Received Date/Time** - In this area, the following fields can be used to specify the event range by the date and time the event was received by Discovery Server:
  - **From** - The beginning of the range of events to filter. Possible values: **First Record** (selected by default) and **Records On**. Select **First Record** to filter events starting from the earliest received one. Select **Records On** to filter events received no earlier than a specific date and time.
  - **To** - The end of the range of events to filter. Possible values: **Last Record** (selected by default) and **Records On**. Select **Last Record** to filter events up to the latest received one. Select **Records On** to filter events received no later than a specific date and time.

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

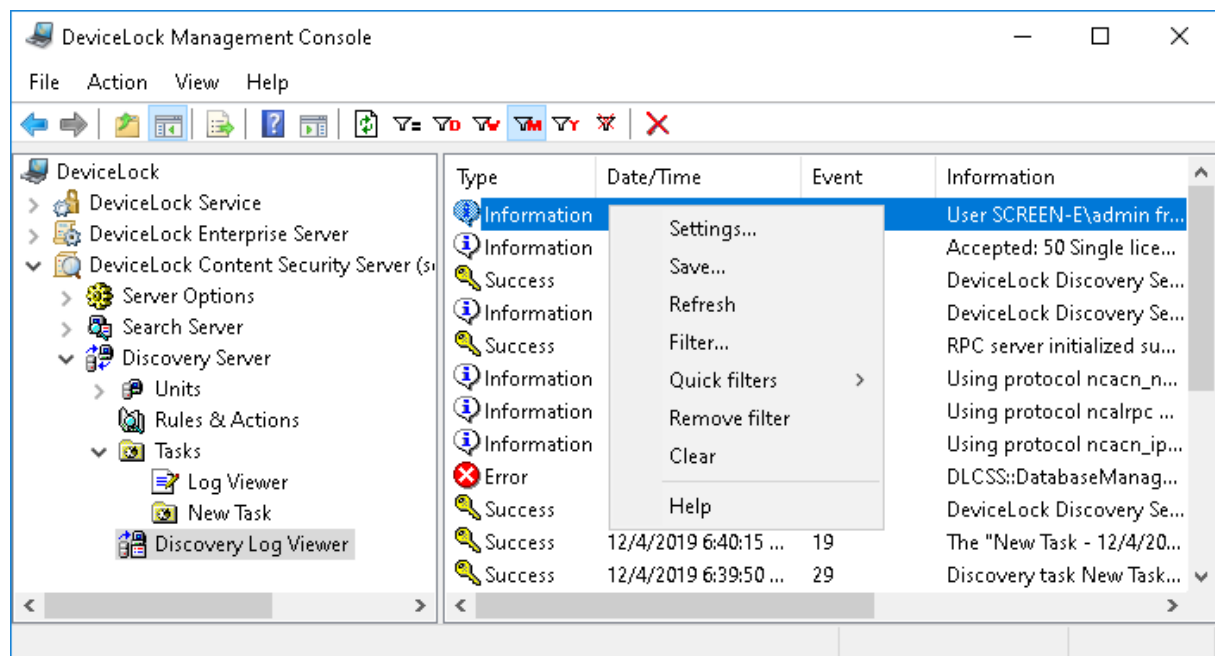
# Discovery Log Viewer

This viewer allows you to retrieve DeviceLock Discovery Server's internal log. The server uses this log to record errors, warnings and other important information (such as configuration changes, start/stop events, and so on). Unlike the Tasks Log, the Discovery Log contains information that has no direct relation to scanning tasks.

You may use the information from this log to diagnose problems (if any), to monitor changes in the server's configuration and to see who has cleared logs and when.

To access the DeviceLock Discovery Server log, do the following:

1. Open the DeviceLock Management Console.
2. In the console tree, expand **DeviceLock Content Security Server > Discovery Server**, and then select **Discovery Log Viewer** under the **Discovery Server** node.



The details pane displays a list of events, with the following information on each event:

- **Type** - Event type indicates one of the following:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Date/Time** - The date and time that the event occurred.
- **Event** - ID number of the event.
- **Information** - Detailed description of the event that includes details of the actions performed and errors encountered.







- **Server** - Identifies the computer on which the event has occurred.
- **Record N** - Sequence number of the event record in the list.

## Managing the Discovery Log

You can manage the log by using commands from the shortcut menu:



- In the console tree, expand **DeviceLock Content Security Server > Discovery Server**, and then right-click **Discovery Log Viewer** under the **Discovery Server** node.  
- OR -
- In the console tree, select **DeviceLock Content Security Server > Discovery Server > Discovery Log Viewer**, and then right-click any list record in the details pane.

The shortcut menu provides the following log management commands (next to the command name is the toolbar button corresponding to that command):

- **Settings** - View or change the settings that limit the maximum number of event records the log may contain. For instructions, see [To view or change Discovery log settings](#).
- **Save** - Saves the log to the file you specify.
- **Refresh**  - Updates the list of events with the latest information.
- **Filter**  - Displays only the events that match the conditions set. For instructions, see [To configure the Discovery log filter](#).
- **Quick filters** - Choose from the following options to display only records for a certain period of time:
  - Current day 
  - Current week 
  - Current month 
  - Current year 

To cancel the quick filter that has been applied, select the same filter option again or use the **Remove filter** command.

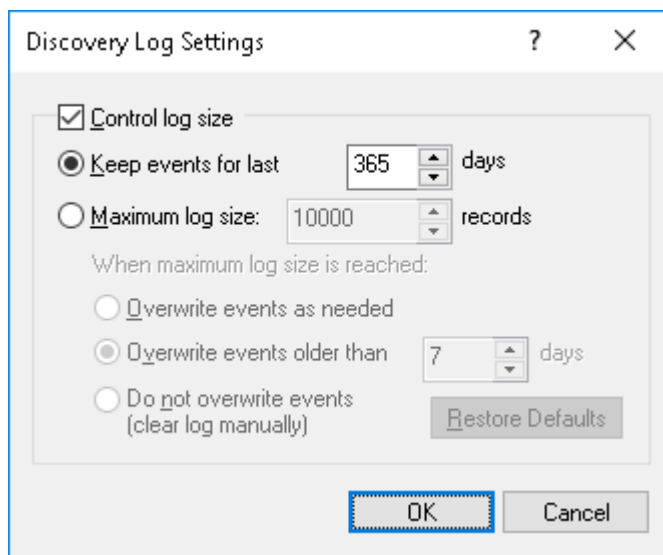
A regular filter enabled by the **Filter** command disables quick filters, and cancels the current quick filter (if any was applied). To enable quick filters, disable the regular filter (for example, by using the **Remove filter** command).

- **Remove filter**  - Show all records by disabling the currently applied filter.
- **Clear**  - Delete all records that currently exist in the log.

This command also adds a deletion record to the log, indicating how many records have been deleted as well as who performed the deletion and from what computer.

### ***To view or change Discovery log settings***

1. Click **Settings** on the shortcut menu.
2. View or change log settings in the dialog box that appears.



The following log settings are available:

- **Control log size** - Select this check box to allow the server to control the number of records in the log and delete outdated records. If this check box is cleared, the server uses all available database space to store the log.
- **Keep events for last <number> days** - Store records no older than a certain number of days. Then, specify the desired number of days. The default setting is 365 days.
- **Maximum log size: <number> records** - Store no more than a certain number of records. Then, specify the desired number of records, and select the server action to be performed when the log reaches the maximum size:
  - **Overwrite events as needed** - New event records continue to be stored when the maximum log size is reached. Each record of a new event replaces the oldest record in the log.
  - **Overwrite events older than <number> days** - New event records replace only records stored longer than the number of days specified. The supported setting is up to 32,767 days.
  - **Do not overwrite events (clear log manually)** - New event records are not added when the maximum log size is reached. To enable the server to add new records, the log must be cleared by hand.

---

### Important

If the log has no space for new records and log settings do not allow the deletion of old records, then the server does not add any new records to the log.

---

To use the default log size, select the option **Maximum log size** and click **Restore Defaults**. The default log size settings are as follows:

- Maximum log size: 10,000 records
- Overwrite events older than 7 days

### *To configure the Discovery log filter*

1. Click **Filter** on the shortcut menu.
2. View or change filter settings in the dialog box that appears.

Two filter types are available:

- **Include** - The console displays only the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Include** tab.
- **Exclude** - The console does not display the events that match these conditions. To set up and apply these conditions, select the **Enable filter** check box on the **Exclude** tab.

The filter can be temporarily disabled by clearing the **Enable filter** check box.

---

#### Note

The mark next to the tab name turns green if the filter on that tab is enabled. Otherwise, the mark is gray.

---

When the filter enabled, its conditions are defined by entering values into the following fields:

- **Event types** - Select check boxes to filter events by type:
  - **Success** - Task or operation completed successfully.
  - **Information** - Certain action performed.
  - **Warning** - A problem might occur unless action is taken.
  - **Error** - A problem has occurred.
- **Information, Server, Event ID** - Include or exclude events depending upon whether event data matches the filter string specified. For example, to filter events by the name of the computer on which the event occurred, specify a filter string in the **Server** field. To filter events with certain

IDs, enter ID numbers separated by a semicolon in the **Event ID** field.

---

**Note**

To assist with configuring a filter, string setting fields store previous entries and suggest matches for what is being typed. Previous entries are also available on the drop-down list of options for the setting field.

---

- **From** - The beginning of the range of events to filter. Possible values: **First Record** (selected by default) or **Records On**. Select **First Record** to filter events from the earliest one in the log. Select **Records On** to filter events that occurred no earlier than a specific date and time.
- **To** - The end of the range of events to filter. Possible values: **Last Record** (selected by default) or **Records On**. Select **Last Record** to filter events up to the latest one in the log. Select **Records On** to filter events that occurred no later than a specific date and time.

When configuring a filter, consider the following:

- Filter conditions are combined by AND logic, that is, a given record matches the filter if it matches each of the filter conditions. Clear the fields that are not to be used in the filter conditions.
- Filter string fields may include wildcards, such as an asterisk (\*) or a question mark (?). An asterisk represents zero or more characters; a question mark represents any single character.
- A filter string field may include multiple values separated by a semicolon (;). In this case, the values are combined by OR logic, that is, a given record matches the filter condition on a particular field if it matches at least one of the values specified in that field.
- The **Clear** button in the **Filter** dialog box provides the option to remove all the defined filter conditions and start setting up a new filter from scratch.
- The **Save** and **Load** buttons in the **Filter** dialog box are used to save the filter conditions to a file and to load previously saved filter conditions from a file.

# Index

“

“Audit” Rights Category 232  
“Encrypted” Rights Category 224  
“Generic” Rights Category 222  
“Shadowing” Rights Category 233  
“Special Permissions” Rights Category 224

## A

About DeviceLock License Types 764  
About logical operators 723  
About Versioning Threshold 358  
Access Control 283, 296  
Access Rights 389  
Access type(s) 692  
Acronis patented technologies 11  
Activating Client Licenses 765  
Activating Server Licenses 766  
Active Directory 664  
Adding Filters 861  
Adding Fingerprints Manually 372  
Administering DeviceLock Content Security Server 704  
Administering DeviceLock Enterprise Server 575  
Administering Digital Fingerprints 360  
Administering the Consolidation of Logs 600  
Administrative Alerts 206  
Alerts 191, 842

## Alerts Settings

Delivery retry parameters 205, 850  
SMTP 197, 846  
SNMP 192, 843  
Syslog 202, 849

Allowed & Denied access requests per channel 666

Allowed vs. Denied access requests 666

Always show tray icon 176

AND/OR operators 723

Anti-keylogger 210

## Appendix

Activating DeviceLock Licenses 764

Consolidating the Logs in the Cloud Using OpenVPN 768

Examples 777

Apply Content-Aware Rules to file/folder names 180

Applying Digital Fingerprints 377

Archives content inspection on read 177

Archives content inspection on write 177

Audit & Shadowing Examples 791

Audit and Shadowing Rights 401

Audit folder operations 188

Audit Log Filter (Server) 582

Audit Log Filter (Service) 263

Audit Log Reports 665

Audit log settings 189

Audit Log Settings (Server) 580

Audit Log Settings (Service) 261

- Audit log threshold for file operations (seconds) 186
- Audit log type 188
- Audit Log Viewer 129
- Audit Log Viewer (Server) 578
- Audit Log Viewer (Service) 258
- Auditing & Shadowing 184
- Auditing, Shadowing & Alerts (Regular Profile) 228
- Auditing, Shadowing & Alerts Dialog Box 230
- Auditing, Shadowing and Alerts Management Tasks 420
- Automating search operations 748

## B

- Basic IP Firewall blocked message 166
- Basic IP Firewall Rule Examples 802
- Basic Security Rules 31
- Binary Files Content Inspection 178
- BlackBerry 234
- Block keyboard 211
- Bluetooth 235

## C

- Career Search 389, 402
- Career Search Services 433
- Changing the Policy Object for a Client Computer 635
- Checking the status of the current indexing actions 717
- Cleanup files older than (days) 187
- Clipboard 235

- Command-line options to sign a settings file 152
- Command Line Utility 59
- Comparing Data 135
- Completing configuration 78, 94, 825
- Complex Content Groups 334
- Complex groups 737
- Computer(s) 688
- Configure the DeviceLock Enterprise Server 771, 775
- Configure the OpenVPN Client 774
- Configure the OpenVPN Server 770
- Configuring access to the DeviceLock Content Security Server 708, 830
- Configuring authentication 602
- Configuring Content Groups 307
- Configuring E-mail Delivery of Reports 698
- Configuring log options 836
- Configuring Offline Mode Detection Settings 460
- Configuring On-premises Servers 772
- Configuring the Cloud Server 769
- Configuring the TCP Port setting 711, 833
- Connecting to Computers 99
- Consolidating Logs 599
- Consolidation server list 603
- Contact(s) 685
- Content-Aware blocked read message 162
- Content-Aware blocked write message 163
- Content-Aware Detection 291, 303
- Content-Aware Rule Examples 797
- Content-Aware Rules (Regular Profile) 280



- Content-Aware Rules Node 281, 294
- Content-Aware Shadowing 288, 300
- Content Inspection 427
- Content verification complete message 171
- Content verification message 169
- ContentLock and NetworkLock 23
- ContentLock and NetworkLock Licensing 28
- Copied files per channel 676
- Copying Content-Aware Rules 350
- Copying firewall rules 449
- Copying offline Content-Aware Rules 491, 533
- Copying offline firewall rules 522
- Copying rules of offline Protocols White List 514
- Copying rules of Protocols White List 437
- Copyright statement 11
- Create/Edit Task 609
- Creating a Custom Policy Object 631
- Creating a filter
  - Example 864
- Creating a Task 884
- Creating a Unit 854
- Creating and configuring a new search task 750
- Creating Custom File Type Detection Groups 309
- Creating Custom Keywords Groups 315
- Creating Custom Pattern Groups 321
- Creating or editing a saved query 726
- Creating or Modifying a Policy 105
- Creating rules 550
- Creating Tasks 362, 683

## D

- Database settings 73, 89, 821
- Default Audit and Shadowing 417
- Default Permissions 227, 395
- Default Policy 630
- Defining and changing offline Security Settings 496, 538
- Defining and changing Security Settings 456
- Defining and editing audit and shadowing rules 421
- Defining and editing offline audit and shadowing rules 468, 505
- Defining and editing offline Media White List 479
- Defining and editing offline USB Devices White List 473
- Defining and Editing Rules and Actions 874
- Defining Audit and Shadowing Rules 230
- Defining Content-Aware Rules 340
- Defining firewall rules 446
- Defining offline Content-Aware Rules 486, 527
- Defining offline firewall rules 519
- Defining offline Protocols White List 510
- Defining Protocols White List 433
- Defining Rules for Devices 341
- Defining Rules for Protocols 345
- Deleted Shadow Data Log 592
- Deleting a Custom Policy Object 633
- Deleting Content-Aware Rules 353
- Deleting firewall rules 453
- Deleting offline Content-Aware Rules 494, 536

- Deleting offline firewall rules 525
- Deleting Reports 703
- Deleting rules of offline Protocols White List 516
- Deleting rules of Protocols White List 440
- Deploying DeviceLock Service for Mac 56
- Deploying DeviceLock Service for Windows 36
- Details table 894
- Device Code 149
- Device type(s) 692
- DeviceLock Administrators 181
- DeviceLock certificate 173
- DeviceLock Certificates 142
- DeviceLock Consoles and Tools 96
- DeviceLock Content Security Server 21, 704
- DeviceLock Discovery Overview 805
- DeviceLock Enterprise Manager 116
- DeviceLock Enterprise Server 575
- DeviceLock Enterprise Server Policies 623
- DeviceLock Enterprise Server(s) 172, 378
- DeviceLock Group Policy Manager 106
- DeviceLock Management Console 96
- DeviceLock Overview 12
- DeviceLock policy changes 673
- DeviceLock Reports 643
- DeviceLock root node 97
- DeviceLock Security Policies (Offline Profile) 459
- DeviceLock Service 157
- DeviceLock Service for Mac 20
- DeviceLock Service node 99
- DeviceLock Service Settings Editor 103
- DeviceLock Service versions 671
- DeviceLock Service versions by computers 672
- DeviceLock Signing Tool 148
- Devices blocked read message 167
- Devices blocked write message 168
- Devices Node 216
- Dialog box for configuring a Digital Fingerprints group 379
- Dialog box for configuring a rule 551
- Dialog box for configuring a task 363
- Dialog box for configuring report options 684
- Dialog box for configuring task schedule and options 694
- Dialog box for managing rules 550
- Dialog box for managing search groups 728
- Digital Fingerprinting Technique 355
- Digital Fingerprints 355
- Digital Fingerprints Content Groups 379
- Direction 444
- Directory Service Connection Settings 663
- Directory service connection settings dialog box 664
- Discovery Log Viewer 902
- Discovery results 893
- Discovery Server 767, 853
- Discovery Server Options 834
- Document Properties Content Groups 326
- Document Properties groups 734
- Domain and User Statistics 647
- Domain Statistics 647
- Duplicating Built-in Content Groups 338

## **E**

Editing a Policy Object 633

Editing Content-Aware Rules 349

Editing firewall rules 448

Editing offline Content-Aware Rules 490, 532

Editing offline firewall rules 521

Editing offline Protocols White List 513

Editing or Deleting Custom Content Groups 338

Editing Protocols White List 436

Elasticsearch Units 868

Enable local storage quota 186

Enabling alerts 423

Enabling Alerts 240

Enabling binary files content inspection 841

Enabling NTLM authentication for local users on Mac OS X 275

Enabling offline alerts 470, 507

Encryption 213

Endpoint Scanning 853

Enterprise Server 766

EtherSensor Server 181

Event folding 651

Examples of user activity monitoring rules 560

Exclude external contact(s) 687

Exclude internal user(s) 686

Executing Search Queries 23

Expired message 161

Exporting and Importing Content-Aware Rules 351

Exporting and importing firewall rules 450

Exporting and importing offline Content-Aware Rules 492, 534

Exporting and importing offline firewall rules 523

Exporting and importing offline Media White List 482

Exporting and importing offline Protocols White List 515

Exporting and importing offline USB Devices White List 476

Exporting and importing Protocols White List 438

Exporting and importing tasks 755

Exporting and Saving Reports 701

## **F**

Failed to scan 894

Fast servers first 175

Features and Benefits 805

File Formats Indexed for Search 761

File name 690

File Sharing 390, 403

File Sharing Services 430

File Type Detection Content Groups 307

File Type Detection groups 729

Filter control dialog box for Elasticsearch 870

Filtering Data 140

Filtering the list of sessions 567

Filtering the log 759

Fingerprinting Options 361

Fingerprinting Tasks 362

Fingerprints Collection and Storage 357

Fingerprints Database 367

- Fingerprints Log Filter 375
- Fingerprints Log Settings 375
- Fingerprints Log Viewer 373
- Fingerprints Matching 359
- Firewall Management Tasks 445
- Firewall Rule Parameters 442
- Firewall Rules 442
- FireWire port 235
- Floppy 235
- FTP 390, 404

## G

- General Information 12, 842
- General Settings 829
- Generating DeviceLock Certificates 143
- Generating Reports 700
- Getting Started Using Digital Fingerprints 360
- Getting Started Using the Consolidation of Logs 599
- Getting started with DeviceLock Group Policy Manager 108
- Getting Started with User Activity Monitor 545
- Getting started with user dossiers 652
- Grayscale 547

## H

- Hard disk 236
- Hosts 428, 444
- How DeviceLock Discovery Works 809
- How Group Policy is applied 107
- How It Works 355
- How Policies Are Processed and Applied 623

- How Search Server Works 22
- HTTP 390, 404

## I

- IBM Notes 391, 405
- ICQ Messenger 391, 406
- If this rule triggers 427, 444
- Immediately Applying Policies to Client Computers 634
- Importing and Exporting Rules 880
- Include internal user(s) 685
- Indexing DeviceLock Enterprise Server Data 22
- Infrared port 236
- Inspecting fingerprints within archives 359
- Inspection and Control of SSL-encrypted Traffic 457
- Install OpenVPN 769, 772
- Install Service 129
- Installation Steps 65
- Installation via DeviceLock Enterprise Manager 45
- Installation via DeviceLock Enterprise Server 54
- Installation via DeviceLock Management Console 45
- Installation via Group Policy 47
- Installation via Microsoft Systems Management Server 45
- Installing DeviceLock 33
- Installing DeviceLock Content Security Server 80, 812
- Installing DeviceLock Discovery 812
- Installing DeviceLock Discovery licenses 836

Installing DeviceLock Enterprise Server 64  
Installing Management Consoles 60  
Installing or removing a DeviceLock  
certificate 710, 833  
Installing Search Server licenses 712  
Installing/Removing DeviceLock Certificate 145  
Interacting with a Graph 649  
Interactive Installation 37, 56  
Interface 97, 117  
Introducing DeviceLock Discovery 805  
Introduction to User Activity Monitor 545  
iPhone 236  
IRC 391, 407

## **J**

Jabber 391, 407

## **K**

Keystroke recording viewer 569  
Keywords Content Groups 312  
Keywords groups 730

## **L**

License information 72, 88, 820  
Licensing 811  
Links to the log viewer 895  
List of Content-Aware Rules for Devices 282  
List of Content-Aware Rules for Protocols 295  
List of Monitoring Sessions 566  
Loading signed settings file on Mac 155  
Loading signed settings file on Windows 153  
Local sender Email(s) 431

Local sender ID(s) 430  
Local storage directory 185  
Local storage quota 571  
Local storage quota (%) 187  
Log consolidation settings 600  
Log event 211  
Log passwords 548  
Log Policy changes and Start/Stop events 173

## **M**

Mail.ru Agent 392, 408  
Managed Access Control 15  
Managing a task and its reports 755  
Managing Audit, Shadowing and Alerts for  
Protocols 401  
Managing Basic IP Firewall 441  
Managing Classifications 366  
Managing Computers Assigned to Policy  
Objects 634  
Managing Content-Aware Rules 340  
Managing content-aware search groups 727  
Managing DeviceLock Policies 626  
Managing DeviceLock Service for Mac 274  
Managing DeviceLock Service for Windows 157  
Managing existing rules 563  
Managing existing tasks 753  
Managing Existing Tasks 364, 695  
Managing General Settings 706  
Managing log settings 758  
Managing Offline Audit, Shadowing and Alerts  
for Devices 467

Managing Offline Audit, Shadowing and Alerts for Protocols 504

Managing Offline Content-Aware Rules for Devices 485

Managing Offline Content-Aware Rules for Protocols 527

Managing Offline IP Firewall 518

Managing Offline Media White List 479

Managing Offline Permissions for Devices 463

Managing Offline Permissions for Protocols 500

Managing Offline Protocols White List 509

Managing Offline Security Policies for Devices 462

Managing Offline Security Policies for Protocols 500

Managing Offline Security Settings for Devices 495

Managing Offline Security Settings for Protocols 538

Managing Offline USB Devices White List 472

Managing Permissions for Protocols 389

Managing Policy Objects 631

Managing Protocols White List 425

Managing saved queries 726

Managing Search Server Settings 712

Managing Security Settings for Protocols 453

Managing Server Options 577

Managing Shadow Log Records 267, 586

Managing the Audit Log (Server) 579

Managing the Audit Log (Service) 260

Managing the database connection settings 711, 834

Managing the Deleted Shadow Data Log 592

Managing the Discovery Log 903

Managing the Fingerprints Log 374

Managing the Monitoring Log 618

Managing the Policy Log 637

Managing the Server Log 594

Managing the Shadow Log (Server) 587

Managing the Shadow Log (Service) 271

Managing the Tasks Log 897

Managing the UAM Log 570

Managing Units 865

MAPI 392, 409

Media Database 252

Media White List (Regular Profile) 248

Media White List Dialog Box 251

Monitoring 604

Monitoring Algorithm 608

Monitoring Log Filter 619

Monitoring Log Settings 619

Monitoring Log Viewer 616

Monitoring Settings 546

Monitoring Tasks 605

MTP 236

Multiple displays 548

## N

Name 443

Navigating Discovery Server 827

Navigating Reports 893

Notify user 211

## O

Offline mode detection 178  
Open / Save / Export 134  
Optical Drive 237  
Options 547  
Override Protocols Permissions 443  
Overview 382, 459, 541, 623  
OWA server(s) 180

## P

Palm 237  
Parallel port 237  
Pattern Content Groups 319  
Pattern groups 732  
Pause while inactive 547  
Perform Configuration and Complete Installation 83, 814  
Performing a search 720  
Permission and Audit Examples for Devices 777  
Permission Examples 777  
Permission Examples for Protocols 794  
Permission Management Tasks 397  
Permissions (Regular Profile) 217  
Permissions Dialog Box 220  
Plug-ins 128  
Policy Application Scenarios  
    Required Configuration Steps 624  
Policy Log Filter 639  
Policy Log Settings 638  
Policy Object 628

Policy Source(s) 174  
Ports 430, 445  
Possible connection errors 102  
Prepare the Client Certificate and IP Address 772  
Prepare the Server Certificates 769  
Prepare to Install 80, 812  
Prevent data transfer on errors 188  
Printer 238  
Printer(s) 691  
Process list 569  
Protocol 443  
Protocol(s) 692  
Protocols (Regular Profile) 382  
Protocols blocked message 165  
Protocols Node 388  
PS/2 keyboard scrambling 212

## R

Read & Write access requests per device type 667  
Rebuilding the index on demand 716  
Recognizing Boldon James Classifier Labels 333  
Recommendations 108  
Refreshing a List of Assigned Computers and Policy Execution Information 635  
Refreshing Lists of Reports 700  
Refreshing the list of events, saving and clearing the log 761  
Relations chart 662  
Relations Chart Node 650  
Relations Chart Report 650

- Relations Charts 644
- Remote recipient Email(s) 432
- Remote recipient ID(s) 431
- Removable 238
- Removing a Client Computer from All Policy Objects 635
- Removing offline audit and shadowing rules 471, 509
- Removing offline Content-Aware Rules 495, 537
- Removing offline firewall rules 526
- Removing offline Media White List 484
- Removing offline permissions 466, 504
- Removing offline Protocols White List 518
- Removing offline Security Settings 499, 540
- Removing offline USB Devices White List 478
- Report Categories and Types 643
- Report Creation Tasks 682
- Report Devices 691
- Report period 684
- Report Permissions/Auditing 129
- Report PnP Devices 131
- Report Protocols 692
- Report TS Devices as regular devices 692
- Reporting period selector 658
- Requirements Overview 768
- Resetting Alert Settings to Defaults 852
- Resetting Individual Settings 852
- Restoring the Default Settings for the Default Policy Object 634
- Retry parameters 602
- Rules 549, 895

- Rules & Actions Node 872
- Rules and Actions 872
- Rules for Devices 280
- Rules for Protocols 293

## S

- Safe file overwrite 188
- Scan agent system requirements 810
- Scan Network Dialog Box 119
- Scanning a network share
  - Example 865
- Screen recording viewer 568
- Search Server 767
- Search Server Options 706
- Security Settings (Regular Profile) 254
- Security Settings Description 255, 454
- Security Settings Management Tasks 455
- Security Settings Node 254
- Selecting Computers 120
- Selecting Plug-ins 126
- Sending Reports by E-mail 702
- Serial port 238
- Server Administrators 577, 705
- Server administrators and certificate 70, 86, 817
- Server Log Filter 596
- Server Log Settings 595
- Server Log Viewer 593
- Server Options 576, 705
- Service account and connection settings 68, 83, 814
- Service Options 158



Service Options for Digital Fingerprints 377  
 Service Settings 150  
 Session Viewer 568  
 Set Service Settings 132  
 Setting and editing offline permissions 464, 501  
 Setting and editing permissions 397  
 Setting Default Format for Reports 699  
 Setting Permissions 220  
 Setting Port 125  
 Setting the data collection interval 841  
 Setting the service startup account 709, 832  
 Setting up alert and notification messages 837  
 Setting Up Discovery Server 827  
 Setting up indexing schedule 715  
 Setting up merge operations schedule 715  
 Setting up the index to include text data from binary files 714  
 Setting up the search query 750  
 Setting up the search schedule and results settings 752  
 Setting up triggering criteria 554  
 Settings file save options 106  
 Shadow Log Filter (Server) 589  
 Shadow Log Filter (Service) 271  
 Shadow Log Reports 675  
 Shadow Log Settings (Server) 588  
 Shadow Log Viewer 133  
 Shadow Log Viewer (Server) 585  
 Shadow Log Viewer (Service) 265  
 Shadow zero-length files 187  
 Skype 392, 410  
 SMB 392, 411  
 SMTP 393, 411  
 Social Networks 393, 412, 432  
 Specifying DeviceLock Enterprise Server/s to index 713  
 Specifying Digital Fingerprints Database Server (s) 835  
 Specifying mail server for Search Server reports 718  
 Specifying Search Server index location 714  
 SSL 430  
 Standard GPO inheritance rules 107  
 Start Installation 82, 813  
 Starting a Scan 127  
 Starting the service 69  
 Starting the Service 85, 816  
 Steps to perform a search 724  
 Store shadow files in the database 78  
 Summary of Audit and Shadowing Rights by Device Type 234  
 Supplying Credentials 124  
 Switching Between Online and Offline Mode 462  
 Syslog settings 189  
 System Requirements 33  
 System state criteria vs. event criteria 558

**T**

Tape 238  
 Task and Its Monitored Computers 606  
 Task and Its Reports 887  
 Tasks 881

Tasks Log Viewer 895

Tasks Node 882

Telegram 393, 412

Telnet 394, 413

Temporary White List 541

Temporary White List Authorization Tool 542

Test

- Connect the Console to the Cloud Server 775

Test Connection 76, 92, 823

Testing Content Groups 339

Threshold 691

Top active computers 668, 677

Top active processes 668, 678

Top active users 669, 679

Top computers 693

Top copied files 679

Top copied files by extension 675, 680

Top files 694

Top inserted USB & FireWire devices 670

Top printed documents 674, 681, 694

Top Printers 693

Top processes 694

Top USB and FireWire devices 693

Top USB devices 693

Top used Printers 673

Top used USB devices 671

Top users 693

Torrent 394, 414

Traffic priority 176

Transfer shadow data to server 190

Treat any USB hub as keylogger 211

TS Devices 238

Type 443

## U

UAM Licensing 30

UAM log filter 572

UAM log settings 571

Unattended Installation 43, 59

Undefining audit and shadowing rules 424

Undefining Content-Aware Rules 353

Undefining firewall rules 452

Undefining offline audit and shadowing rules 471, 508

Undefining offline Content-Aware Rules 494, 537

Undefining offline firewall rules 526

Undefining offline media White List 484

Undefining offline permissions 466, 503

Undefining offline Protocols White List 517

Undefining offline Security Settings 498, 539

Undefining offline USB Devices White List 478

Undefining permissions 400

Undefining Protocols White List 439

Undefining Security Settings 456

Understanding DeviceLock Discovery 805

Uninstall Service 133

Unique Contact Statistics 648

Units 853

Updating the existing index on demand 716

USB Devices Database 247

USB Devices White List (Regular Profile) 241

- USB Devices White List Dialog Box 244
- USB port 239
- USB/FireWire blocked message 160
- Use global DeviceLock Enterprise Server(s) settings 378
- Use Group/Server Policy 174
- User account information 653
- User action details 660
- User activity charts 659
- User Activity Monitor 545
- User Activity Monitor (UAM) 29
- User activity overview 656
- User Card 653
- User Dossiers 650
- User ID Statistics 648
- User List 652
- User loyalty indicator 654
- User(s) 690
- Using DeviceLock Group Policy Manager 111
- Using Group Policy to Manage DeviceLock Service for Mac 116
- Using Log Viewers 578
- Using Resultant Set of Policy (RSoP) 114
- Using Search Server 719
- Using the “Edit Rule” dialog box 877
- Using the “Rules & Actions” dialog box 875
- Using the Policies Node 627
- Using the Policy Log Viewer 636

## V

- Version(s) 690
- Versioning threshold for binary 361

- Versioning threshold for text 361
- Viber 394, 414
- Video resolution 548
- Viewing a Report 889
- Viewing a task's report 756
- Viewing and managing the tasks log 757
- Viewing Built-in Content Groups 337
- Viewing Detailed Fingerprint Information 370
- Viewing Fingerprint List 368
- Viewing Report Parameters 701
- Viewing Reports 701
- Viewing Reports Created by a Task 696
- Viewing Task Run Reports 366
- Viewing the report list 888
- Viewing User Activity 565

## W

- Ways to stop recording 559
- Web Mail 394, 415
- Web Mail Services 432
- Web Search 394, 415
- Web Search Services 432
- What if a rule triggers when recording is in progress? 562
- What If Server's Fingerprints Database Is Unavailable to Client? 359
- What if there is nothing to record? 563
- WhatsApp 394, 415
- White-Listed Devices 243
- White-Listed Media 250
- White List Management Tasks 433
- White List Rule Parameters 426

White List Rules 425

WiFi 239

Windows Mobile 239

Working with Reports 699

Working with search results 738

Working with shadow copies 747

## **Z**

Zoom 395, 416