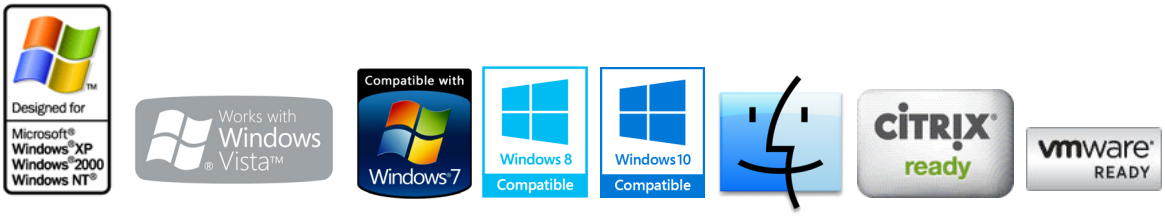
DeviceLock®

AN ACRONIS COMPANY

Acronis DeviceLock DLP 9.0

Руководство пользователя



© 1996-2021 АО «Смарт Лайн Инк». Все права защищены.

Сведения, приведенные в этом документе, могут быть изменены в любой момент без предварительного уведомления. В целях обеспечения авторских прав никакая часть настоящего документа ни в каких целях за исключением личных некоммерческих целей не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, если на то нет предварительного письменного разрешения компании АО «Смарт Лайн Инк».

Товарные знаки

DeviceLock и логотип DeviceLock являются зарегистрированными товарными знаками компании АО «Смарт Лайн Инк». Все другие названия продуктов, услуг и товарных знаков, упомянутые в данном документе, являются товарными знаками соответствующих владельцев.

Acronis DeviceLock DLP - Руководство пользователя
Версия продукта: 9.0
Обновлено: июнь 2021

Содержание

Об этом руководстве 8
Условные обозначения 8

Краткий обзор DeviceLock 9
Основная информация 9
Управляемый контроль доступа 14
Сервис DeviceLock для Mac 18
Сервер DeviceLock Content Security Server 19
Как работает поисковый сервер 19
Модули ContentLock и NetworkLock 21
Лицензирование NetworkLock и ContentLock 26
Модуль мониторинга активности пользователей 27
Лицензирование модуля UAM 28
Правила обеспечения безопасности 29

Установка DeviceLock 30
Системные требования 30
Развертывание сервиса DeviceLock для Windows 34
Интерактивная установка 34
Установка без вмешательства пользователя 39
Установка с помощью Systems Management Server 40
Установка в DeviceLock Management Console 40
Установка в DeviceLock Enterprise Manager 41
Установка через групповые политики 42
Установка с помощью DeviceLock Enterprise Server 49
Развертывание сервиса DeviceLock для Mac 50
Интерактивная установка 50
Использование командной строки 52
Установка без вмешательства пользователя 53
Установка консолей управления 54
Установка DeviceLock Enterprise Server 58
Инструкции по установке 58
Установка DeviceLock Content Security Server 72
Подготовка к установке 72
Запуск установки 74
Настройка и завершение установки 75

Консоли и инструменты DeviceLock 87
DeviceLock Management Console 87
Пользовательский интерфейс 88
Подключение к компьютеру 91
DeviceLock Service Settings Editor 95
Создание или редактирование политики 96
DeviceLock Group Policy Manager 98
О применении групповых политик 98
Начало работы с DeviceLock Group Policy Manager 100
Использование DeviceLock Group Policy Manager 103
Использование Resultant Set of Policy (RSoP) 106
Управления сервисом DeviceLock для Mac через групповые политики 107
DeviceLock Enterprise Manager 108
Пользовательский интерфейс 109

Диалоговое окно “Сканирование сети” 110
Модули 118
Загрузка / Сохранение / Экспорт 125
Сравнение данных 126
Фильтрация данных 130
Сертификаты DeviceLock 133
Создание сертификата 133
Установка и удаление сертификата 135
Мастер создания подписи 138
Код устройства 139
Настройки сервиса 140

Сервис DeviceLock 145
Управление сервисом DeviceLock для Windows 145
Настройки сервиса 147
Узел “Устройства” 200
Разрешения (обычный профиль) 201
Аудит, теневое копирование и алерты (обычный профиль) 213
Белый список USB-устройств (обычный профиль) 228
Белый список носителей (обычный профиль) 235
Настройки безопасности (обычный профиль) 240
Просмотрщик журнала аудита (для компьютера) 244
Просмотрщик журнала теневого копирования (для компьютера) 251
Управление сервисом DeviceLock для Mac 259
Разрешение NTLM-аутентификации для локальных пользователей в Mac OS X 260

Контентно-зависимые правила (обычный профиль) 264
Правила для устройств 264
Узел “Контентно-зависимые правила” 265
Управление доступом к контенту 268
Теневое копирование контента 274
Обнаружение контента 277
Правила для протоколов 279
Узел “Контентно-зависимые правила” 280
Управление доступом к контенту 283
Теневое копирование контента 286
Обнаружение контента 290
Настройка контентных групп 294
Группы определения типа файла 295
Группы ключевых слов 299
Группы шаблонов 307
Группы свойств документа 314
Составные группы 323
Просмотр встроенных контентных групп 326
Дублирование встроенных контентных групп 327
Редактирование или удаление пользовательских контентных групп 328
Тестирование контентных групп 329
Управление контентно-зависимыми правилами 330
Создание контентно-зависимых правил 330
Редактирование контентно-зависимых правил 339
Копирование контентно-зависимых правил 340
Экспорт и импорт контентно-зависимых правил 342
Сброс контентно-зависимых правил в исходное состояние 344
Удаление контентно-зависимых правил 345

Цифровые отпечатки 346
О методе цифровых отпечатков 346
Как этот метод устроен 347
Сбор и хранение отпечатков 349
Сравнение отпечатков 350
Приступая к работе с цифровыми отпечатками 352
Управление цифровыми отпечатками 353
Настройки отпечатков 353
Задачи отпечатков 354
База отпечатков 360
Журнал отпечатков 366
Применение цифровых отпечатков 371
Настройки сервиса для цифровых отпечатков 371
Группы цифровых отпечатков 372

Протоколы (обычный профиль) 375
Общая информация 375
Узел “Протоколы” 381
Разрешения на доступ к протоколам 382
Права доступа 382
Разрешения по умолчанию 389
Действия по управлению разрешениями 391
Аудит, теневое копирование и алерты для протоколов 396
Права аудита и теневого копирования 397
Аудит и теневое копирование по умолчанию 417
Действия по управлению аудитом, теневым копированием и алертами 420
Белый список протоколов 425
Правила белого списка 426
Параметры правил белого списка 427
Действия по управлению белым списком 434
Базовый IP-файрвол 443
Правила файрвола 444
Параметры правил файрвола 445
Действия по управлению файрволом 448
Настройки безопасности для протоколов 457
Описание настроек безопасности 458
Действия по управлению настройками безопасности 459
Контроль трафика с SSL-шифрованием 461

Политики безопасности DeviceLock (офлайн-профиль) 462
Общая информация 462
Настройка конфигурации для автономного режима 464
Переключение между оперативным и автономным режимами 466
Управление политиками безопасности для автономного режима (устройства) 467
Управление разрешениями 468
Управление правилами аудита, теневого копирования и оповещений 474
Управление белым списком USB-устройств 481
Управление белым списком носителей 489
Управление контентно-зависимыми правилами 497
Управление настройками безопасности 511
Управление политиками безопасности для автономного режима (протоколы) 517
Управление разрешениями 517
Управление правилами аудита, теневого копирования и оповещений 523
Управление белым списком протоколов 530
Управление базовым IP-файрволом 541

Управление контентно-зависимыми правилами 553
Управление настройками безопасности 566

Временный белый список 570
Общая информация 570
Получение временного доступа 571

Мониторинг активности пользователей 573
Общие сведения 573
Приступая к работе с мониторингом активности пользователей 574
Настройки мониторинга 575
Параметры 575
Правила 578
Просмотр активности пользователей 595
Список сеансов мониторинга 596
Просмотр сеанса мониторинга 597
Управление журналом активности пользователей 600

Сервер DeviceLock Enterprise Server 605
Администрирование сервера DeviceLock Enterprise Server 605
Настройки сервера 606
Средства просмотра журналов DeviceLock 609
Просмотрщик журнала аудита (для сервера) 609
Просмотрщик журнала теневого копирования (для сервера) 617
Просмотрщик журнала сервера 625
Консолидация журналов 630
Приступая к работе с консолидацией журналов 631
Управление консолидацией журналов 632
Мониторинг 637
Задачи мониторинга 638
Просмотрщик журнала мониторинга 649

Политики DeviceLock Enterprise Server 654
Общая информация 654
Как обрабатываются и применяются политики 654
Сценарии применения политик: пошаговое конфигурирование 656
Управление политиками DeviceLock 659
Использование узла “Политики” 659
Управление объектами политики 664
Управление компьютерами, назначенными объектам политики 669
Просмотр журнала политик 672

Отчеты в DeviceLock 677
Категории и типы отчетов 677
Графы связей 678
Пользовательские досье 685
Отчеты по данным журнала аудита 701
Отчеты по данным журнала теневого копирования 715
Задачи создания отчетов 723
Создание задач 724
Управление существующими задачами 736
Просмотр отчетов, созданных задачей 737
Настройка электронной почты для доставки отчетов 739
Выбор формата отчетов по умолчанию 740
Работа с отчетами 741

Создание отчетов 741
Обновление списков отчетов 742
Просмотр отчетов 742
Просмотр параметров отчета 743
Экспорт и сохранение отчетов 743
Отправка отчетов по электронной почте 744
Удаление отчетов 745

Сервер DeviceLock Content Security Server 746
Администрирование сервера DeviceLock Content Security Server 746
Настройки сервера 747
Управление общими параметрами сервера 749
Управление параметрами поискового сервера 755
Использование поискового сервера 762
Выполнение поиска 762
Работа с результатами поиска 783
Автоматизация поиска 792
Типы файлов, индексируемых для поиска 806

Приложение: Активация лицензий DeviceLock 809
О типах лицензий DeviceLock 809
Активация клиентских лицензий 811
Активация серверных лицензий 812
Enterprise Server 812
Поисковый сервер 812
Сервер Discovery 813

Приложение: Консолидация журналов в облаке с помощью OpenVPN 814
Обзор требований 814
Настройка облачного сервера 815
Установить OpenVPN 815
Подготовить сертификаты сервера 816
Настроить сервер OpenVPN 817
Настроить DeviceLock Enterprise Server 818
Настройка локальных серверов 818
Установить OpenVPN 818
Подготовить клиентский сертификат и IP-адрес 819
Настроить клиент OpenVPN 820
Настроить DeviceLock Enterprise Server 821
Тест: Подключить консоль к облачному серверу 821

Приложение: Примеры 822
Примеры разрешений и правил аудита для устройств 822
Примеры разрешений 822
Примеры правил аудита и теневого копирования 836
Примеры разрешений для протоколов 839
Примеры контентно-зависимых правил 842
Примеры правил IP-файрвола 848

Об этом руководстве

В данном руководстве содержится подробная информация по установке и использованию Acronis DeviceLock DLP. Документ предназначен в первую очередь для сетевых администраторов, специалистов по безопасности данных и других ИТ-специалистов, которые заинтересованы в обеспечении безопасности корпоративных данных.

Использование руководства подразумевает, что читатель знаком с основами управления установленной операционной системой и имеет базовые понятия о настройке локальной сети.

Условные обозначения

В руководстве используются следующие условные обозначения.

Элемент	Описание
Полужирный шрифт	Обозначает элементы пользовательского интерфейса.
Курсив	Используется для комментариев.
Голубой шрифт	Используется для выделения гиперссылок.
Примечание	Дополнительная информация об описываемых процессах.
Полезный совет	Рекомендации для получения наилучших результатов.
Внимание	Действия, которые следует выполнять с большой осторожностью.
Знак “плюс” (+)	Указывает на сочетание клавиш, которые надо нажимать одновременно.

1

Краткий обзор DeviceLock

В этой главе:

Основная информация

Управляемый контроль доступа

Сервис DeviceLock для Mac

Сервер DeviceLock Content Security Server

Модули ContentLock и NetworkLock

Модуль мониторинга активности пользователей

Правила обеспечения безопасности

Основная информация

Наиболее эффективный подход к защите от утечек информации с компьютеров начинается с использования, прежде всего, механизмов контекстного контроля - запрета или разрешения передачи данных для конкретных пользователей в зависимости от форматов данных, типов интерфейсов и устройств, сетевых протоколов, направления передачи, дня недели и времени суток и т.д.

Однако, во многих случаях требуется более глубокий уровень контроля - например, проверка содержимого передаваемых данных на наличие персональной или конфиденциальной информации в условиях, когда порты ввода-вывода не должны блокироваться, чтобы не нарушать производственные процессы, но отдельные пользователи входят в «группу риска», поскольку подозреваются в причастности к нарушениям корпоративной политики информационной безопасности. В подобных ситуациях дополнительно к контекстному контролю необходимо применение технологий контентного анализа и фильтрации, позволяющих выявить и предотвратить передачу неавторизованных данных, не препятствуя при этом информационному обмену в рамках служебных обязанностей сотрудников.

Программный комплекс DeviceLock DLP использует как контекстные, так и основанные на анализе контента методы контроля данных, обеспечивая надежную защиту от информационных утечек с пользовательских компьютеров и серверов корпоративных ИС при минимальных затратах на приобретение и обслуживание комплекса. Контекстные механизмы DeviceLock реализуют гранулированный контроль доступа пользователей к широкому спектру периферийных устройств и каналов ввода-вывода, включая сетевые коммуникации. Дальнейшее повышение уровня защиты достигается за счет применения методов контентного анализа и фильтрации данных, что позволяет предотвратить их несанкционированное копирование на внешние накопители и Plug-and-Play устройства, а также передачу по сетевым протоколам за пределы корпоративной сети.

Наряду с методами активного контроля эффективность применения DeviceLock обеспечивается за счет детального протоколирования действий пользователей и административного персонала, а также селективного теневого копирования передаваемых данных для их последующего анализа, в том числе с использованием методов полнотекстового поиска.

Программный комплекс DeviceLock DLP состоит из взаимодополняющих функциональных модулей - DeviceLock, NetworkLock, ContentLock, DeviceLock Search Server (DLSS) и DeviceLock Discovery, лицензируемых опционально в любых комбинациях для удовлетворения задач служб информационной безопасности.

Базисный компонент DeviceLock является инфраструктурной платформой и ядром для других компонентов комплекса и реализует все функции его централизованного управления и администрирования. DeviceLock поддерживает полный набор механизмов контекстного контроля доступа пользователей, а также обеспечивает событийное протоколирование (аудит) и теневое копирование данных для всех локальных каналов ввода-вывода на защищаемых компьютерах, включая периферийные устройства и интерфейсы, системный буфер обмена, локально подсоединенные смартфоны и КПК, Media Transfer Protocol (MTP), а также канал печати документов на локальные и сетевые принтеры. Кроме того, компонент DeviceLock включает в себя все консоли централизованного управления.

Компонент NetworkLock™ обеспечивает контекстный контроль каналов сетевых коммуникаций на рабочих компьютерах, включая распознавание сетевых протоколов независимо от используемых портов, детектирование коммуникационных приложений и их селективную блокировку, реконструкцию сессий с восстановлением файлов, данных и параметров, а также событийное протоколирование и теневое копирование передаваемых данных.

NetworkLock контролирует большинство популярных сетевых протоколов и приложений, включая простые и SSL-защищенные SMTP-сессии электронной почты (с раздельным контролем сообщений и вложений), взаимодействие между клиентом Microsoft Outlook и сервером Microsoft Exchange (протокол MAPI), IBM Notes, веб-доступ и другие HTTP приложения, включая HTTPS сессии, веб-службы электронной почты и социальные сети (AOL Mail, freenet.de, Gmail, GMX Mail, Hotmail (Outlook.com), Mail.ru, NAVER, Outlook Web App (OWA), Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail, Zimbra; Facebook, Google+, Instagram, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, Pinterest, StudiVZ, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru), службы мгновенных сообщений (Skype, Telegram, Viber, WhatsApp, ICQ Messenger, Jabber, IRC, Mail.ru Агент), облачные хранилища (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive и др.), передачу файлов по протоколам FTP и FTP-SSL, передачу файлов в локальной сети по SMB, а также сеансы Telnet и Torrent.

Компонент ContentLock™ реализует механизмы контентного мониторинга и фильтрации файлов и данных, передаваемых с/на сменные носители и в каналах сетевых коммуникаций - веб-почте и социальных сетях, службах мгновенных сообщений, файловом обмене по протоколам FTP и FTP-SSL и др. Кроме того, технологии контентной фильтрации в модуле ContentLock позволяют задать фильтрацию для данных теневого копирования, чтобы сохранять только те файлы и данные, которые информационно значимы для задач аудита информационной безопасности, расследований нештатных ситуаций и их криминалистического анализа.

Компонент DeviceLock Search Server (DLSS) обеспечивает полнотекстовый поиск по централизованным базам данных теневого копирования и событийного протоколирования. Сервер DLSS позволяет значительно снизить трудозатратность и повысить эффективность процессов аудита и расследования инцидентов информационной безопасности, связанных с утечками информации, их криминалистического анализа и сбора доказательной базы. DeviceLock Search Server может автоматически распознавать, индексировать, находить и отображать документы множества форматов, таких как: Adobe Acrobat (включая зашифрованные файлы, если шифрование файла выполнено одним из следующих алгоритмов: 40-bit RC4, 128-bit RC4, 128-bit AES и 256-bit AES, и при этом разрешения, установленные на файл, не запрещают извлечение текста) (PDF), Ami Pro, AutoCAD (DWG, DXF), Архивы (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Visio, Microsoft Word, Microsoft Works, OpenOffice (документы, таблицы и презентации), Quattro Pro, WordPerfect, WordStar и многие другие.

Компонент DeviceLock Discovery выполняет сканирование рабочих станций и корпоративных сетевых ресурсов, и на основании заданных политик способен обнаруживать документы и файлы с критическим содержимым, осуществлять различные действия с обнаруженными документами, а также может инициировать процедуры управления инцидентами, направляя тревожные оповещения в реальном режиме времени. Подробную информацию о DeviceLock Discovery можно найти в документе “Руководство пользователя DeviceLock Discovery”.

Помимо обеспечения контроля доступа к портам, устройствам и каналам сетевых коммуникаций, включая событийное протоколирование (аудит), DeviceLock обеспечивает тревожные оповещения безопасности (алерты) в реальном времени, уведомляя администратора о серьезных происшествиях и проблемах. Оповещения в реальном времени упрощают отслеживание событий в журнале, а также позволяют оперативнее и более эффективно реагировать на инциденты и нарушения политики безопасности. Оповещения отправляются по протоколам SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol) и/или syslog.

Функция теневого копирования в DeviceLock позволяет для каждого пользователя или группы сохранять точную копию данных, копируемых на внешние устройства, передаваемых по сети и через последовательные и параллельные порты, а также печатаемых на локальных и сетевых принтерах. Точные копии всех файлов и данных сохраняются в SQL-базе данных. Теневое копирование, как и аудит, может быть задано для отдельных пользователей и групп пользователей.

Кроме того, теневое копирование DeviceLock совместимо с библиотекой программного обеспечения, поддерживаемой национальным институтом стандартов и технологий США, а также с базой данных Hashkeeper, созданной и поддерживаемой министерством юстиции США.

Данные теневого копирования могут быть проверены на вхождение в базы данных известных файлов, что позволяет их использовать в компьютерной криминалистике.

Такие базы данных содержат цифровые “отпечатки” множества известных файлов (файлы операционных систем, прикладного программного обеспечения и т.п.). Вы можете создать ваши собственные базы данных цифровых “отпечатков” (поддерживаются алгоритмы SHA-1, MD5 и CRC32) конфиденциальных файлов и затем использовать их для выявления фактов копирования пользователями этих конфиденциальных файлов.

За дополнительной информацией об использовании DeviceLock с базами данных цифровых “отпечатков” обращайтесь в службу технической поддержки DeviceLock.

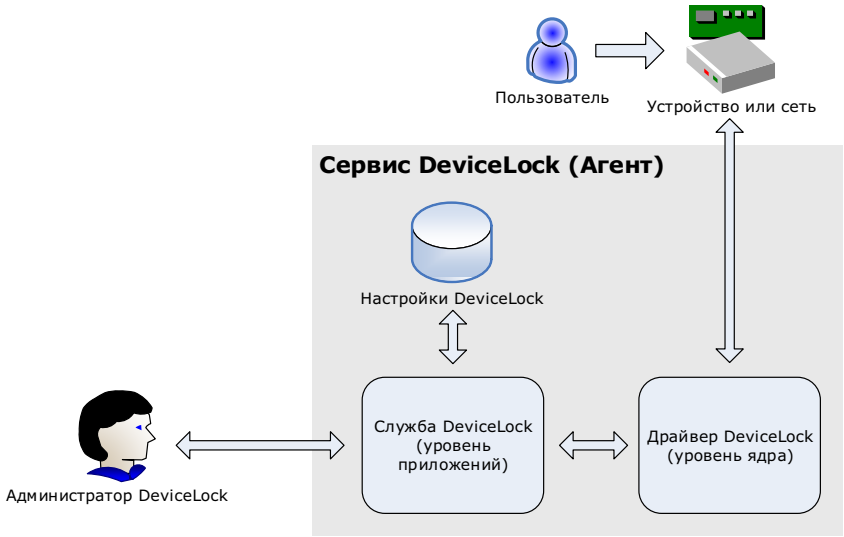
Дополнительную информацию о базах данных цифровых “отпечатков” известных файлов, а также примеры подобных баз данных можно найти на сайте национального института стандартов и технологий США по адресу www.nsrl.nist.gov.

В дополнение к стандартным возможностям управления правами доступа и настройками, DeviceLock предлагает наиболее рациональный и удобный подход к управлению DLP-системой - с использованием объектов групповых политик домена Microsoft Active Directory и интегрированной в редактор групповых политик (GPO Editor) консоли DeviceLock. При этом политики DeviceLock автоматически распространяются средствами директории как интегральная часть ее групповых политик на все компьютеры домена. Такое решение позволяет службе информационной безопасности централизованно и оперативно управлять DLP-политиками в масштабах всей организации, а их исполнение распределенными агентами DeviceLock обеспечивает точное соответствие между бизнес-функциями пользователей и их правами на передачу и хранение информации на рабочих компьютерах.

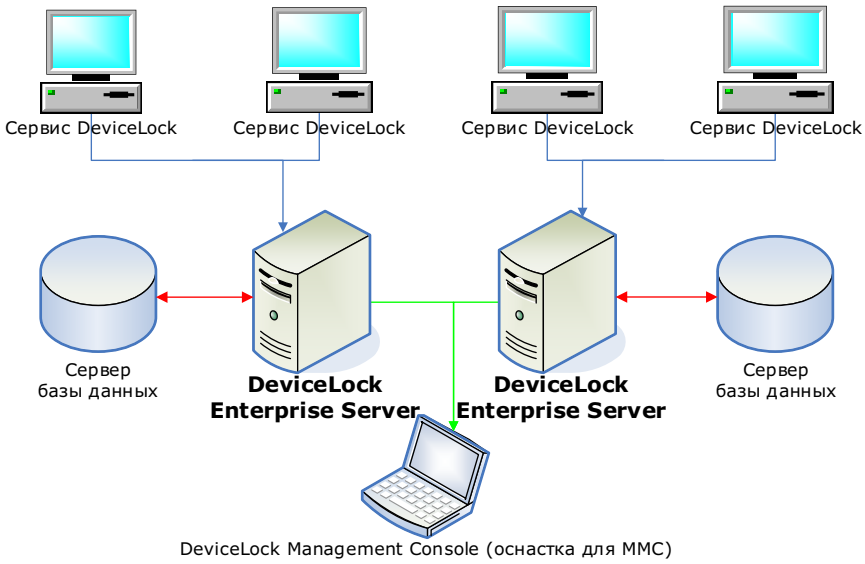
Глубокая интеграция в Active Directory - важная особенность DeviceLock. Она упрощает развертывание в больших сетях и более удобна для системных администраторов, а также исключает необходимость установки дополнительных приложений для централизованного управления и развертывания. Полная интеграция централизованного управления DeviceLock в групповые политики Windows позволяет автоматически устанавливать DeviceLock на новые компьютеры, подключаемые к корпоративной сети, и осуществлять настройку политик контроля доступа, аудита и теневого копирования и других настроек Агентов DeviceLock для новых компьютеров в автоматическом режиме. DeviceLock не требует своего собственного серверного компонента для контроля за всей сетью, вместо этого используется стандартная функция, предоставляемая Active Directory.

В состав программного комплекса DeviceLock DLP входят три основные части: агент (сервис DeviceLock), серверы (DeviceLock Enterprise Server и DeviceLock Content Security Server) и консоли управления (DeviceLock Management Console, DeviceLock Group Policy Manager и DeviceLock Enterprise Manager).

1. Агент DeviceLock, или сервис DeviceLock - это ядро системы DeviceLock. Агент устанавливается на каждый контролируемый компьютер, автоматически запускается и обеспечивает защиту устройств и сети на машине-клиенте, оставаясь в то же время невидимым для локального пользователя.

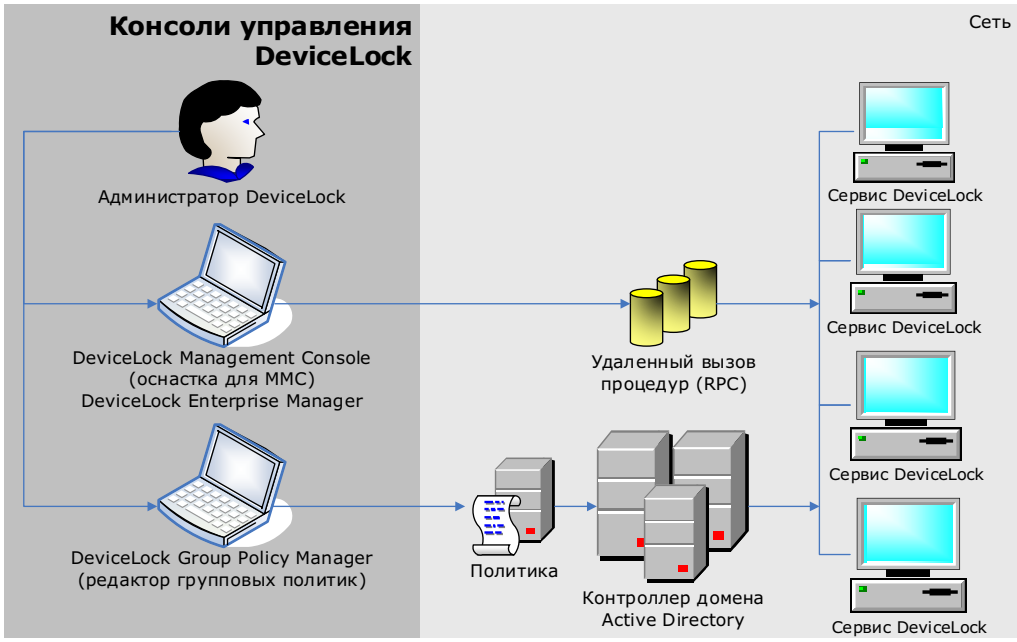


2. DeviceLock Enterprise Server (DLES) - это дополнительный компонент, предназначенный для централизованного сбора и хранения данных теневого копирования и журналов аудита. Для хранения своих данных DeviceLock Enterprise Server использует сервер базы данных - SQL Server или PostgreSQL. Для равномерного распределения нагрузки в локальной сети можно установить несколько экземпляров DLES и серверов базы данных.



DeviceLock Content Security Server - еще один дополнительный компонент, включающий в себя компонент Search Server для быстрого поиска текста в файлах теневого копирования и журналах, хранящихся на DeviceLock Enterprise Server. Дополнительную информацию см. в разделе Сервер DeviceLock Content Security Server ниже в этой главе.

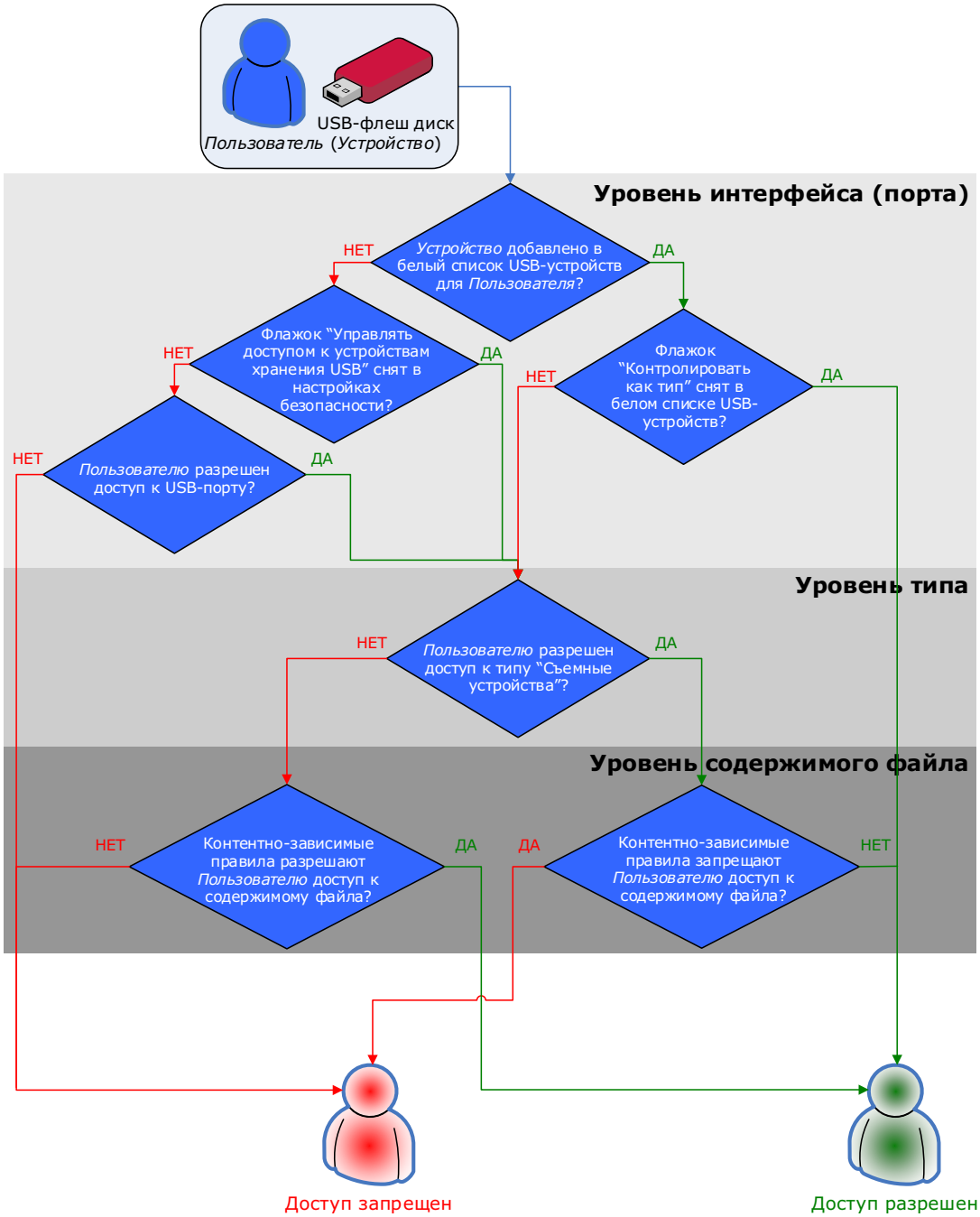
3. Консоль управления - это интерфейс контроля, который системный администратор использует для удаленного управления любой системой, на которой установлен сервис DeviceLock. DeviceLock поставляется с четырьмя консолями управления: DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Group Policy Manager (интегрируется в редактор групповых политик Windows). DeviceLock Management Console также используется для управления серверами DeviceLock Enterprise Server и Content Security Server.



Управляемый контроль доступа

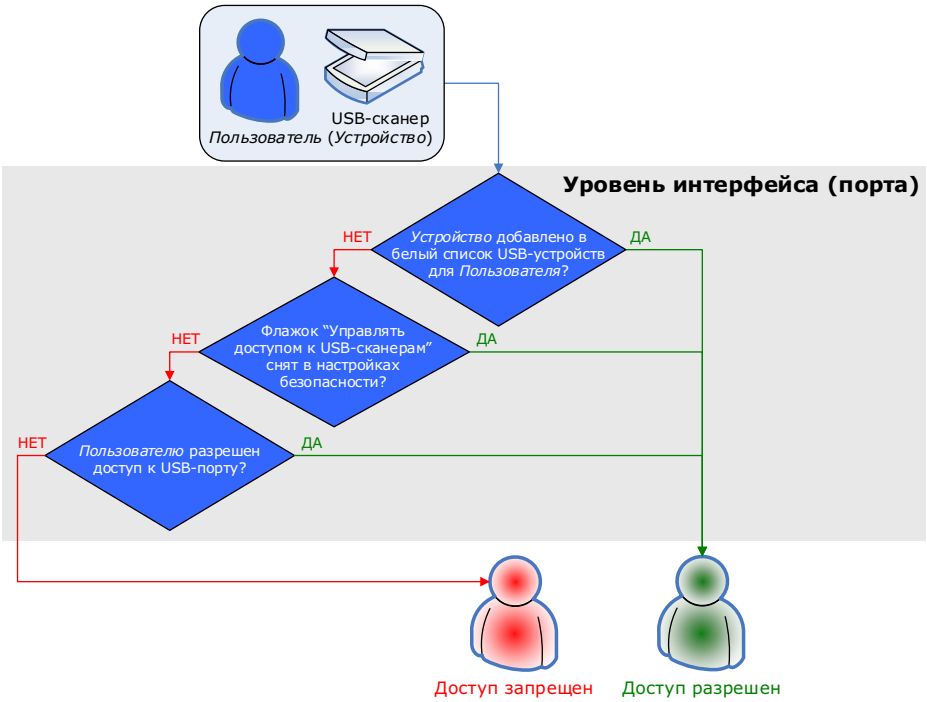
Контроль доступа для устройств работает следующим образом: каждый раз, когда пользователь пытается получить доступ к устройству, DeviceLock перехватывает запрос на уровне ядра ОС. В зависимости от типа устройства и интерфейса подключения (например, USB), DeviceLock проверяет права пользователя в соответствующем списке управления доступом (ACL). Если у пользователя отсутствуют права доступа к данному устройству, будет возвращено сообщение об ошибке “доступ запрещен”.

Проверка разрешений на доступ выполняется на трех уровнях: интерфейс (порт), тип и содержимое файла. Некоторые устройства проверяются на всех трех уровнях, в то время как другие - только на одном: либо на уровне интерфейса (порта), либо на уровне типа.



Рассмотрим случай доступа пользователя к USB-флеш через USB-порт. В данном случае DeviceLock в первую очередь проверит на уровне интерфейса (USB-порта), открыт или нет доступ к USB-порту. Затем, поскольку Windows определяет USB-флеш как съемное устройство, DeviceLock также проверит ограничения на уровне типа устройства (съемное). И в завершение проверки DeviceLock также проверит ограничения на уровне содержимого файла, определенные контентно-зависимыми правилами.

В случае же использования USB-сканера доступ будет проверяться только на уровне интерфейса (USB-порта), поскольку DeviceLock не имеет отдельного типа устройств для сканеров.



Существуют дополнительные настройки безопасности (см. Настройки безопасности (обычный профиль)), которые могут выключать контроль доступа для классов устройств (напр., для всех USB-клавиатур и мышей), в то время как остальные устройства остаются под контролем. В этом случае, если устройство принадлежит к классу, для которого контроль отключен, DeviceLock пропускает все запросы на соединение с этим устройством на уровне интерфейса (порта). DeviceLock также поддерживает белый список определенных устройств (см. Белый список USB-устройств (обычный профиль)); иными словами, вы можете отключить контроль доступа только для определенных устройств (например, некоторых USB-принтеров).

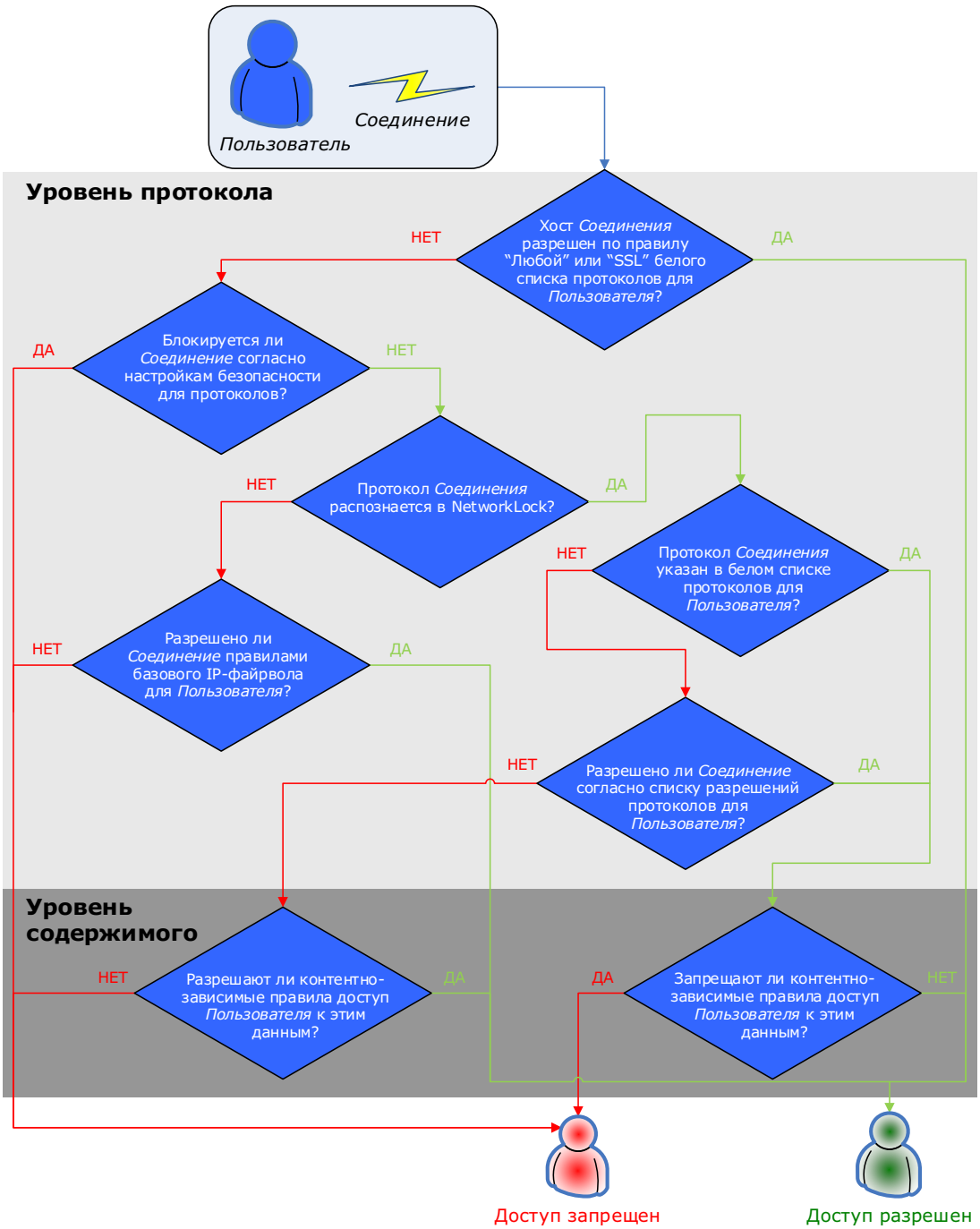
Примечание: Если доступ к устройству запрещен на уровне интерфейса (порта), DeviceLock не будет проверять разрешения на уровне типа. Если доступ к устройству на уровне интерфейса (порта) разрешен, DeviceLock также проверит разрешения на уровне типа. Пользователь может подключиться к устройству, только если у него есть права на обоих уровнях.

Контроль доступа для протоколов работает следующим образом: каждый раз, когда пользователь пытается получить доступ к удаленному сетевому ресурсу, DeviceLock перехватывает запрос на соединение на уровне ядра ОС и проверяет права пользователя в соответствующем списке управления доступом (ACL). Если у пользователя отсутствуют права доступа к данному протоколу, будет возвращено сообщение об ошибке "доступ запрещен".

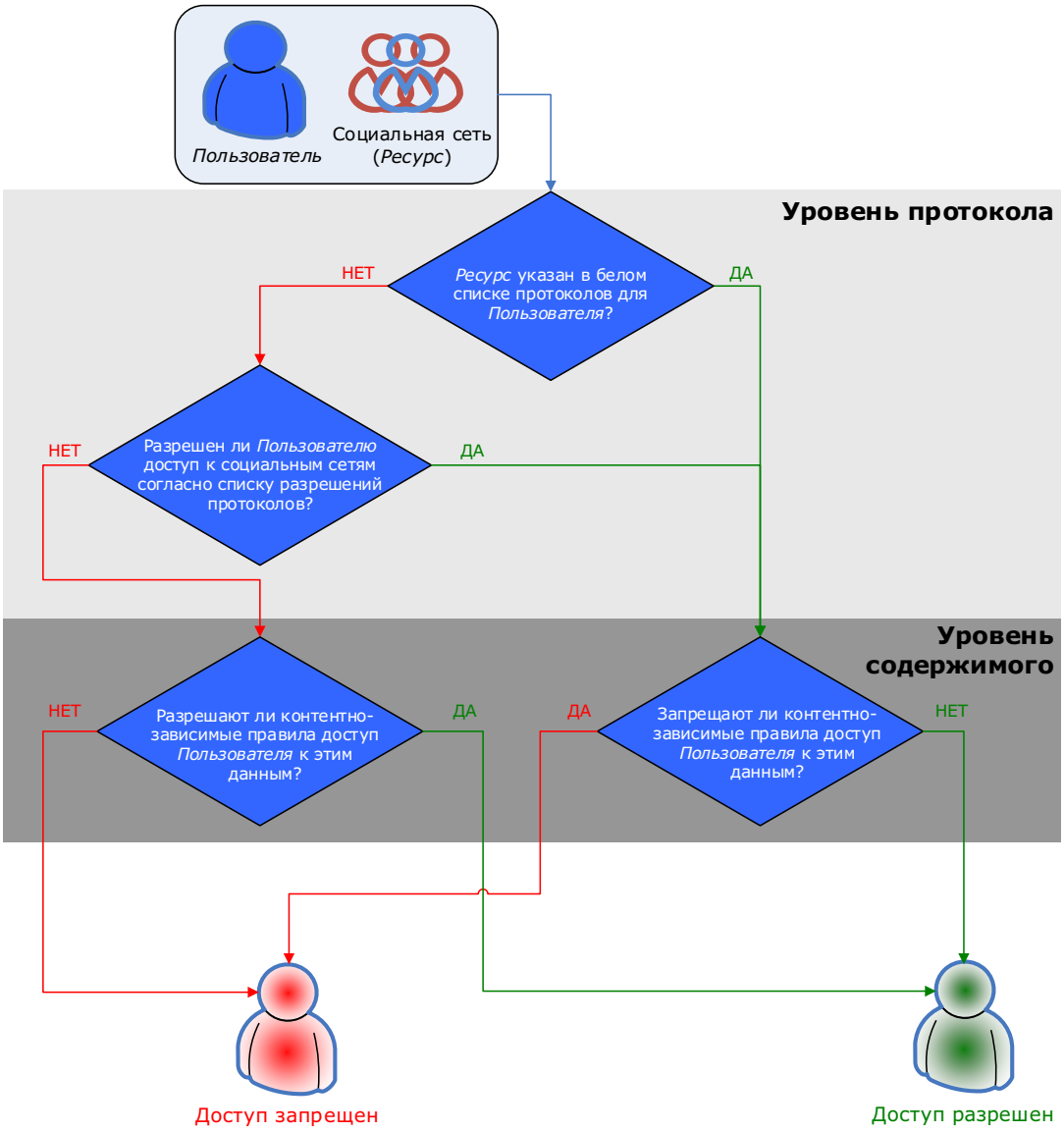
Примечание: Настройки контроля доступа для социальных сетей, сервисов файлового обмена и веб-почты имеют преимущество перед настройками для протокола HTTP. Например, если пользователям разрешен доступ к почтовой службе Gmail, но запрещено использовать протокол HTTP, они, тем не менее, смогут получить доступ к почтовой службе.

Проверка разрешений на доступ выполняется на двух уровнях: протокол и содержимое. Все сетевые подключения проверяются на обоих уровнях, за исключением подключений по протоколам Торрент, Telnet, Telegram и WhatsApp, которые проверяются только на уровне протокола.

Например, при попытке пользователя подключиться к удаленному узлу, DeviceLock проверит, разрешено ли подключение на уровне протокола, а затем будут проверены разрешения на уровне содержимого передаваемых данных, определенные контентно-зависимыми правилами.



Рассмотрим случай доступа пользователя к сайту социальной сети. В данном случае DeviceLock в первую очередь проверит на уровне протокола, открыт или нет доступ к социальным сетям. Затем DeviceLock проверит разрешения на уровне содержимого данных, определенные контентно-зависимыми правилами.



Кроме того, DeviceLock поддерживает белые списки протоколов (см. Белый список протоколов). Белый список протоколов позволяет отключать контроль доступа для сетевых подключений с определенными параметрами (например, HTTP-подключений для определенных узлов и портов).

Сервис DeviceLock для Mac

Сервис DeviceLock для Mac создан, чтобы помочь администраторам и службам информационной безопасности предотвратить неавторизованную передачу данных, блокировать копирование файлов и предотвратить загрузку программного обеспечения.

Благодаря поддержке широкого ряда устройств, носителей и протоколов хранения данных, сервис DeviceLock для Mac обеспечивает гибкий контроль доступа к внутренним и внешним устройствам хранения данных, таким как оптические приводы CD, DVD, BD, внешние накопители и диски; контролирует доступ к адаптерам WiFi и Bluetooth, обеспечивает управляемый контроль доступа к портам USB, FireWire и последовательному порту. Устройства, подключаемые по шине eSATA, контролируются как класс съемных устройств, а устройства, подключаемые по шине Thunderbolt, контролируются как класс съемных устройств и как устройства WiFi.

Сервис DeviceLock для Mac включает следующие функциональные возможности:

- **Контроль доступа к портам и устройствам хранения данных**. С помощью сервиса DeviceLock для Mac администраторы получают полный контроль над тем, кто, когда, и при каких условиях может получить доступ к определенным устройствам и портам. Это позволяет предотвратить утечку данных в том числе и через неавторизованные приложения.
- **Аудит пользовательской активности**. Сервис DeviceLock для Mac позволяет вести подробный аудит активности с конкретных типов устройств на рабочих станциях. Основанная на контексте безопасности пользователя, эта функциональность позволяет администраторам и службам ИБ отслеживать активность отдельных пользователей и групп пользователей. Журналы аудита, создаваемые агентом, собираются сервером DeviceLock Enterprise Server и отображаются в консолях управления.
- **Теневое копирование**. Сервис DeviceLock для Mac позволяет администраторам и службам ИБ просматривать, какая именно информация была передана пользователями путем создания теневых копий всех данных, отправляемых или передаваемых через определенные порты и устройства. Система использует теневое копирование данных для зеркалирования всех данных, копируемых на внешние устройства хранения данных. Точная копия переданных файлов может быть сохранена в SQL-базе данных. Теневое копирование, как и аудит, может быть задано для отдельных пользователей и групп пользователей.
- **Интеграция в Active Directory**. Полная интеграция в Active Directory делает сервис DeviceLock для Mac легко конфигурируемым и управляемым, упрощает настройку параметров агентов, настройку прав доступа и развертывание агентов в больших гетерогенных сетях. Интеграция сервиса DeviceLock для Mac в домен позволяет получать данные для конфигурирования агентов из Active Directory через DeviceLock Enterprise Server.

Сервер DeviceLock Content Security Server

DeviceLock Content Security Server - дополнительный компонент программного комплекса DeviceLock DLP. Он включает в себя поисковый сервер (Search Server), который обеспечивает полнотекстовый поиск по данным журналов, хранящихся на DeviceLock Enterprise Server, что делает управление данными более простым и эффективным на фоне их увеличивающегося количества в базе данных DeviceLock Enterprise Server.

Также DeviceLock Content Security Server включает в себя сервер Discovery, предназначенный для обнаружения документов и файлов с критическим содержимым. Подробную информацию о сервере Discovery можно найти в документе "Руководство пользователя DeviceLock Discovery".

DeviceLock Content Security Server включает следующие функциональные возможности:

- **Поддержка полнотекстового поиска**. Посредством использования поискового сервера DeviceLock Content Security Server позволяет быстро искать важные текстовые данные, применяя различные критерии поиска.
- **Автоматизация операций полнотекстового поиска**. DeviceLock Content Security Server позволяет выполнять поисковые запросы по расписанию с автоматической отправкой результатов поиска по электронной почте.
- **Гибкие настройки конфигурации**. Для оптимизации производительности DeviceLock Content Security Server предусмотрены различные параметры конфигурации.

Полнотекстовый поиск можно использовать для нахождения данных, которые невозможно найти с применением фильтров в просмотрщиках журналов. Полнотекстовый поиск особенно полезен в ситуациях, когда необходимо осуществлять поиск теневых копий документов по их содержимому.

Для управления сервером DeviceLock Content Security Server используется консоль DeviceLock Management Console.

Вариант использования - Предотвращение утечек конфиденциальной информации

Специалисты по безопасности, чьей задачей является оперативное выявление инцидентов, связанных с конфиденциальностью важной информации, могут регулярно использовать поисковый сервер для оперативного и удобного поиска и анализа теневых копий файлов, содержащих важные бизнес-данные, например, списки клиентов или прайс-листы. Записи в журнале, относящиеся к найденным теневым копиям, помогут определить, когда и кем была скопирована конфиденциальная информация. Имея эти данные, специалисты по безопасности могут предпринять оперативные меры для предотвращения возможного раскрытия и утечки информации за пределами компании.

Как работает поисковый сервер

Поисковый сервер выполняет следующие функции:

- Индексирует данные DeviceLock Enterprise Server.
- Выполняет полнотекстовые запросы после операции индексирования.

Более подробное описание этих функций представлено ниже.

Индексирование данных DeviceLock Enterprise Server

Индексирование - это процесс, в результате которого текстовые данные на DeviceLock Enterprise Server становятся доступными для поиска и просмотра.

Поисковый сервер начинает индексирование автоматически, как только будут указаны экземпляры сервера DeviceLock Enterprise Server. В результате процесса индексирования создается или обновляется полнотекстовый индекс. Каждый поисковый сервер создает только один полнотекстовый индекс, что делает управление более эффективным. В полнотекстовом индексе хранятся данные о существенных для поиска словах и их позициях. В процессе создания или обновления индекса поисковый сервер отбрасывает неучитываемые слова (такие, как предлоги, артикли и т.п.), которые не повышают эффективность поиска.

Поисковый сервер индексирует все текстовые данные из следующих источников: журнал аудита, журнал теневого копирования, журнал удаленных данных теневого копирования, внутренний журнал сервера DeviceLock Enterprise Server, журнал мониторинга и журнал политик сервера DeviceLock Enterprise Server.

Процесс индексирования выполняется в два этапа. На первом этапе поисковый сервер извлекает ключевые слова из теневых копий и записей в журналах и сохраняет их во временные индексы для каждого указанного DeviceLock Enterprise Server. Для каждого временного индекса поисковый сервер обрабатывает 1000 записей из каждого журнала. На втором этапе, когда число временных индексов становится равным 50 или проходит 10 минут, инициируется процесс объединения всех временных индексов в один главный полнотекстовый индекс, который используется для поисковых запросов. Процесс объединения временных индексов в главный полнотекстовый индекс называется слиянием (*merging*).

Процесс создания главного полнотекстового индекса требует много времени. Скорость индексирования может значительно изменяться в зависимости от типа индексируемых данных и используемого оборудования. Скорость индексирования обычно находится в диапазоне от 30 до 120 MB/мин. Рассмотрим следующий пример:

- Данные: 170 GB, состоящие из 4 373 004 файлов разного типа (HTML, офисные документы, текстовые файлы)
- Время индексирования: 24.7 часов (6.8 GB/час)
- Размер индекса: 12% от исходного размера документов
- Оборудование: Pentium® 4 Processor 550 (3.40GHz, 800 FSB), 2GB RAM, встроенный SATA RAID-0.

Выполнение поисковых запросов

После того, как данные на DeviceLock Enterprise Server будут проиндексированы, можно выполнять полнотекстовые запросы. Эти запросы могут выполнять поиск по заданным словам или фразам.

При выполнении запроса поисковый сервер обрабатывает его и извлекает из индекса список результатов поиска, соответствующих критериям поискового запроса. Чтобы ограничить количество возвращаемых по поиску результатов, можно использовать фильтрование. Например, результаты поиска могут быть отфильтрованы по типу журнала или дате.

Запросы к полнотекстовому индексу выполняются очень быстро. Операция поиска, в ходе которой находятся и возвращаются совпадения, удовлетворяющие критериям поиска, занимает лишь несколько секунд. Для получения подробной информации о странице результатов поиска и результатах поиска см. раздел Работа с результатами поиска далее в этом документе.

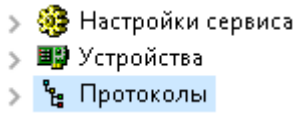
Модули ContentLock и NetworkLock

DeviceLock DLP поставляется с модулями ContentLock и NetworkLock - отдельно лицензируемыми компонентами, обеспечивающими дополнительные функциональные возможности DeviceLock. Эти модули устанавливаются автоматически, но требуют лицензии на использование. Для получения подробной информации о лицензировании модулей ContentLock и NetworkLock см. раздел Лицензирование NetworkLock и ContentLock ниже в этой главе.

Примечание: Компоненты ContentLock и NetworkLock на данный момент не поддерживаются в сервисе DeviceLock для Mac.

Модуль NetworkLock предоставляет дополнительные возможности контекстного контроля сетевых коммуникаций на рабочих компьютерах пользователей. NetworkLock распознает сетевые протоколы независимо от используемых портов, обеспечивает определение приложений и их выборочное блокирование, реконструкцию сообщений и сессий с извлечением файлов, данных и параметров, а также событийное протоколирование и теневое копирование передаваемых данных. NetworkLock контролирует большинство популярных сетевых протоколов и приложений, включая простые и SSL-защищенные SMTP-сессии электронной почты (с раздельным контролем сообщений и вложений), взаимодействие между клиентом Microsoft Outlook и сервером Microsoft Exchange (протокол MAPI), IBM Notes, веб-доступ и другие HTTP приложения, включая HTTPS сессии, веб-службы электронной почты и социальные сети, такие как Gmail, Yahoo! Mail, Windows Live Mail, Facebook, Twitter, LiveJournal и др., службы мгновенных сообщений Skype, Telegram, Viber, WhatsApp, ICQ Messenger, Jabber, IRC, Mail.ru Агент, облачные хранилища (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive и др.), передачу файлов по протоколам FTP и FTP-SSL, передачу файлов в локальной сети по SMB, а также сеансы Telnet и Torrent.

Модуль NetworkLock представлен в виде узла **Протоколы** в пользовательском интерфейсе консолей DeviceLock Management Console, Service Settings Editor и DeviceLock Group Policy Manager:



Модуль NetworkLock имеет следующие функциональные возможности:

- **Контроль доступа к сетевым протоколам**. Позволяет контролировать доступ пользователей и групп пользователей к протоколам FTP, HTTP, SMTP, MAPI (Microsoft Exchange), IBM Notes, SMB, Torrent и Telnet, службам мгновенных сообщений (Skype, Telegram, Viber, WhatsApp, ICQ Messenger, Jabber, IRC, Mail.ru Агент), сайтам веб-поиска, веб-сайтам поиска работы, веб-конференциям и вебинарам (Zoom.us), веб-службам электронной почты и социальным сетям (AOL Mail, freenet.de, Gmail, GMX Mail, Hotmail (Outlook.com), Mail.ru, NAVER, Outlook Web App (OWA), Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail, Zimbra; Facebook, Google+, Instagram, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, Pinterest, StudiVZ, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru) и облачным хранилищам файлов (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive и др.) в зависимости от времени суток и дня недели.
- **Белый список протоколов**. Позволяет выборочно разрешить передачу данных по сети через указанные протоколы, несмотря на установленные настройки блокирования доступа к протоколам. Белый список наиболее эффективен для реализации сценария “минимальные привилегии”, когда администратор блокирует трафик по всем протоколам, а затем предоставляет пользователям минимальные привилегии, необходимые для работы.

- **Контентно-зависимые правила ("Определение типа файла")**. Позволяют выборочно разрешить или запретить доступ к определенным типам файлов, передаваемым по сетевым каналам. Алгоритм определения типов файлов основан исключительно на анализе содержимого файла. Этот надежный алгоритм позволяет идентифицировать файлы и правильно их обрабатывать вне зависимости от расширения файла. Контентно-зависимые правила можно также использовать, чтобы разрешить или запретить теневое копирование определенных типов файлов.

  Примечание: Для доступа к расширенным возможностям, предоставляемым функциональностью контентно-зависимых правил, необходимо приобрести лицензию на модуль ContentLock.

- **Аудит, теневое копирование и оповещения**. Позволяет проводить аудит действий пользователей с протоколами, сохранять полные копии переданных по сети файлов и данных, а также оперативно оповещать администраторов и/или сотрудников информационной безопасности о ненадлежащих действиях пользователей.

Модуль ContentLock - это компонент, обеспечивающий контентную фильтрацию и мониторинг и существенно повышающий функциональные возможности контентно-зависимых правил. ContentLock позволяет разрешать или запрещать доступ к информации, основываясь не только на определении типа файла, но и на шаблонах регулярных выражений (RegExp) с различными численными и логическими условиями соответствия шаблона критериям и ключевым словам. Распознавая более 80 форматов файлов и типов данных, ContentLock извлекает и отфильтровывает содержимое данных, копируемых на внешние устройства хранения данных и передаваемых по сетевым каналам. С помощью ContentLock также можно задать фильтрацию для данных теневого копирования, чтобы сохранять только те файлы и данные, которые могут иметь значение при расследовании инцидентов информационной безопасности и анализе журналов теневого копирования. Это существенно снижает объем данных, хранимых в базе данных теневого копирования, и снижает нагрузку на локальную сеть, вызванную передачей этих данных на сервер с БД теневого копирования.

Модуль ContentLock имеет следующие функциональные возможности:

- **Контентно-зависимый контроль доступа к документам**. Позволяет контролировать доступ к документам, основываясь на их содержимом. Таким образом, можно предотвратить утечку важных данных, одновременно предоставляя авторизованным пользователям доступ к информации, необходимой для их работы.
- **Контентно-зависимая фильтрация данных теневого копирования**. Позволяет сохранять в журнал теневого копирования только критически важную для организации информацию, что существенно снижает объем хранимых на сервере данных и облегчает работу с сохраненными данными.
- **Контроль документов на основе классификации контента**. Позволяет использовать цифровые отпечатки документов, а также классификационные метки приложений Boldon James Classifier для управления разрешениями на доступ/передачу контента, контентно-зависимым созданием теневых копий и/или простым обнаружением контента:
  - Цифровые отпечатки конфиденциальных документов снимаются и хранятся на сервере DeviceLock Enterprise Server. С их помощью можно идентифицировать полные копии и отдельные фрагменты документов, даже если документ был изменен.
  - В приложениях Boldon James Classifier классификационные метки задают уровень секретности документа путем соответствующей установки его атрибутов.
- **Поддержка множества типов файлов и данных**. Позволяет анализировать содержимое файлов и данных следующих типов: Adobe Acrobat (в т.ч. зашифрованные файлы, если шифрование файла выполнено одним из следующих алгоритмов: 40-bit RC4, 128-bit RC4, 128-bit AES и 256-bit AES, и при этом разрешения, установленные на файл, не запрещают извлечение текста) (*.pdf), Adobe Framemaker MIF (*.mif), Ami Pro (*.sam), Ansi-текст (*.txt), ASCII-текст, ASF-файлы (только метаданные) (*.asf) , AutoCAD (*.dwg, *.dxf), CSV (значения, разделённые запятыми) (*.csv), DBF (*.dbf), EBCDIC, EML (сохраненные в Outlook Express письма) (*.eml), Enhanced Metafile Format (*.emf), Eudora MBX-файлы (*.mbx), Flash (*.swf), HTML (*.htm, *.html), iCalendar

(*.ics), Ichitaro (версия 5 и выше) (*.jtd, *.jbw), JPEG (*.jpg), Lotus 1-2-3 (*.123, *.wk?), почтовые архивы MBOX (включая Thunderbird) (*.mbx), MHT-файлы (HTML-архивы, сохраненные Internet Explorer) (*.mht), MIME-сообщения (включая вложения), MSG (сохраненные в Outlook письма) (*.msg), Microsoft Access MDB-файлы (включая Access 2007 и Access 2010) (*.mdb, *.accdb), Microsoft Document Imaging (*.mdi), Microsoft Excel (*.xls), Microsoft Excel 2003 XML (*.xml), Microsoft Excel 2007, 2010 и 2013 (*.xlsx), Microsoft OneNote 2007, 2010 и 2013 (*.one), файлы Microsoft Outlook (*.PST), сообщения, заметки, контакты, встречи и задачи календаря Microsoft Outlook/Exchange, хранилища сообщений Microsoft Outlook Express 5 и 6 (*.dbx), Microsoft PowerPoint (*.ppt), Microsoft PowerPoint 2007, 2010 и 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 для Windows (*.doc), Microsoft Word 2003 XML (*.xml), Microsoft Word 2007, 2010 и 2013 (*.docx), Microsoft Works (*.wks), MP3 (только метаданные) (*.mp3), Multimate Advantage II (*.dox), Multimate версии 4 (*.doc), документы, таблицы и презентации OpenOffice версий 1, 2 и 3 (включает OASIS Open Document Format for Office Applications) (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf), Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw), QuickTime (*.mov, *.m4a, *.m4v), TIFF (только метаданные) (*.tif), TNEF (winmail.dat), Treepad HJT-файлы (*.hjt), Unicode (UCS16, формат Mac или Windows, UTF-8), Visio XML-файлы (*.vdx), Windows Metafile Format (*.wmf), WMA-файлы (только метаданные) (*.wma), WMV-файлы (только метаданные) (*.wmv), WordPerfect 4.2 (*.wpd, *.wpf), WordPerfect (версия 5.0 и выше) (*.wpd, *.wpf), WordStar version 1, 2, 3 (*.ws), WordStar версии 4, 5, 6 (*.ws), WordStar 2000, Write (*.wri), XBase (включая FoxPro, dBase и другие XBase-совместимые форматы) (*.dbf), XML (*.xml), XML Paper Specification (*.xps), XSL, XyWrite, а также PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, EMF Spooled Files и GDI Printing (ZjStream).

Примечание: Анализ содержимого документов AutoCAD (.dwg, .dxf) поддерживается на компьютерах под управлением Windows XP или более поздних версий ОС.

- **Автоматическая защита новых документов**. Позволяет автоматически применять политики безопасности, основанные на контроле содержимого данных, к новым документам сразу после их создания.
- **Различные методы обнаружения контента**. Позволяют обнаруживать и идентифицировать критически важную для организации информацию в документах на основе регулярных выражений, ключевых слов и свойств документов.
- **Централизованное управление контентом**. Контентно-зависимые правила создаются на основе контентных групп, позволяющих централизованно задавать типы контента, которые требуют контроля.
- **Возможность перекрывать политики, заданные на уровне типа устройства/протокола**. Позволяет выборочно разрешить или запретить доступ к определенному содержимому вне зависимости от разрешений, установленных на тип устройства или протокол.
- **Проверка файлов внутри архивов**. Позволяет осуществлять проверку каждого файла, содержащегося в архиве. Используется следующий алгоритм проверки: когда пользователь пытается скопировать архивный файл на устройство или передать его по сети, все файлы извлекаются из архива и анализируются по отдельности с целью обнаружения содержимого, доступ к которому запрещен контентно-зависимыми правилами. Если контентно-зависимые правила запрещают доступ по крайней мере к одному файлу, содержащемуся в архиве, доступ пользователя к архиву будет запрещен. Если контентно-зависимые правила разрешают доступ ко всем файлам, содержащимся в архиве, доступ пользователя к архиву будет разрешен.

Примечание: DeviceLock может не выполнять проверку отпечатков файлов внутри архива, если обнаруживается полного совпадения файла-архива с файлом-источником отпечатка из базы данных. Подробнее об этом см. в разделе Проверка отпечатков внутри архива главы Цифровые отпечатки далее в этом документе.

Все архивированные файлы извлекаются в системную папку `Temp`. Обычно это папка `%windir%\Temp`. Если сервис DeviceLock не имеет доступа к системной папке `Temp`, архивированные файлы не анализируются и доступ к архиву запрещается, если выполняется хотя бы одно из следующих условий:

- Задано запрещающее контентно-зависимое правило.
- Доступ к типу устройства или протоколу запрещен.

Все вложенные архивы также распаковываются и анализируются один за другим. Архивные файлы идентифицируются только по содержимому, а не по расширению. Поддерживаются следующие форматы архивов: 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), а также CramFS, SquashFS (.squashfs), NTFS, FAT и MBR образы файловых систем и дисков. Разделенные на несколько частей (многотомные) архивы и защищенные паролем архивы не распаковываются.

Примечание: Чтобы разрешить передачу разделенных на части (многотомных) архивов при условии, что в разделе Настройки сервиса включен параметр Проверка содержимого архивов при чтении или Проверка содержимого архивов при записи, необходимо создавать разрешающие правила на основе Группы свойств документа с установленным флажком **Извлечение текста не поддерживается**.

- **Оптическое распознавание символов (OCR)**. Позволяет распознавать и извлекать текст из сканированных документов, сфотографированных (под углом 90 градусов к фотографируемой поверхности) документов, а также экранных снимков документов, и проверять его контентно-зависимыми правилами.

  OCR имеет следующие возможности:

  - Целое изображение или некоторые его фрагменты могут быть перевернуты, повернуты или представлены в зеркальном виде.
  - Поддерживаются малоконтрастные и неяркие изображения.
  - Большинство шрифтов распознается с высокой степенью точности.

  OCR имеет следующие ограничения:

  - Распознавание рукописного текста или любых рукописных шрифтов не поддерживается.
  - Эмбоссированные и выгравированные тексты не распознаются.
  - Наилучший результат распознавания достигается на изображениях с текстом черного цвета на белом фоне.

  Встроенный модуль OCR поддерживает следующие языки: арабский, болгарский, каталонский, китайский-традиционный, китайский-упрощенный, корейский, хорватский, чешский, датский, голландский, английский, эстонский, финский, французский, немецкий, венгерский, индонезийский, итальянский, латышский, литовский, норвежский, польский, португальский, румынский, русский, словацкий, словенский, испанский, шведский, турецкий и японский. Поддерживаются следующие типы файлов: BMP, Dr. Halo CUT, DDS, EXR, Raw Fax G3, GIF, HDR, ICO, IFF (за исключением Maya IFF), JBIG, JNG, JPEG/JIF, JPEG-2000, JPEG-2000 codestream, KOALA, Kodak PhotoCD, MNG, PCX, PBM/PGM/PPM, PFM, PNG, Macintosh PICT, Photoshop PSD, RAW camera, Sun RAS, SGI, TARGA, TIFF, WBMP, XBM, XPM.

  Примечание: Функциональность OCR поддерживается только для клиентских компьютеров под управлением Windows XP или более поздних версий ОС.

- **Обнаружение текста на изображении**. Технология обнаружения текста на изображении делит графические файлы на две группы: изображения с текстом (например сканированные документы или экранные снимки документов) и изображения без текста, причем доступ к этим группам контролируется по отдельности. Например, можно разрешить определенным пользователям копирование на устройства изображений, не содержащих текст, но запретить им запись изображений, содержащих текст, и тем самым предотвратить утечку важной информации внутри графических файлов. Поддерживаются следующие типы файлов: BMP, Dr. Halo CUT, DDS, EXR, Raw Fax G3, GIF, HDR, ICO, IFF (за исключением Maya IFF), JBIG, JNG, JPEG/JIF, JPEG-2000, JPEG-2000 codestream, KOALA, Kodak PhotoCD, MNG, PCX, PBM/PGM/PPM, PFM, PNG, Macintosh PICT, Photoshop PSD, RAW camera, Sun RAS, SGI, TARGA, TIFF, WBMP, XBM, XPM.
- **Проверка изображений, встроенных в документы**. Позволяет выполнять проверку каждого изображения, встроенного в файлы сохраненных писем (EML), Adobe Portable Document Format (включая зашифрованные файлы, если шифрование файла выполнено одним из следующих алгоритмов: 40-bit RC4, 128-bit RC4, 128-bit AES и 256-bit AES, и при этом разрешения, установленные на файл, не запрещают извлечение текста) (PDF), Rich Text Format (RTF), документы AutoCAD (.dwg, .dxf) и в документы Microsoft Office (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx). Все встроенные изображения извлекаются из таких документов в папку Temp пользователя System и анализируются независимо от текста с целью обнаружения содержимого, запрещенного контентно-зависимыми правилами. Текст документов проверяется контентно-зависимыми правилами, созданными на основе контентных групп “Ключевые слова”, “Шаблон” или “Составное”. Встроенные изображения проверяются контентно-зависимыми правилами, созданными на основе контентных групп “Ключевые слова”, “Шаблон”, “Определение типа файла”, “Свойства документа” и “Составное”. Доступ к документу разрешается, только если разрешен доступ к тексту и всем графическим изображениям, вставленным в документ.

Примечание: Анализ изображений, встроенных в документы AutoCAD (.dwg, .dxf), поддерживается только для клиентских компьютеров под управлением Windows XP или более поздних версий ОС.

Лицензирование NetworkLock и ContentLock

Чтобы использовать возможности модулей NetworkLock и ContentLock в составе программного комплекса DeviceLock DLP, необходимо приобрести соответствующие лицензии в дополнение к лицензиям на базовый модуль DeviceLock.

Лицензия на модуль NetworkLock позволяет использовать функциональность контроля каналов сетевых коммуникаций (протоколов).

Лицензия на модуль ContentLock позволяет создавать и применять контентно-зависимые правила, используя шаблоны регулярных выражений, ключевые слова и свойства документов, а также создавать и применять сложные правила, используя логические выражения.

Если используются различные типы лицензий, необходимо учитывать следующее:

- Наличие базовой лицензии DeviceLock и лицензий на модули ContentLock и NetworkLock дает возможность использовать функциональность контроля каналов сетевых коммуникаций (протоколов), возможность создавать и применять контентно-зависимые правила, используя шаблоны регулярных выражений, ключевые слова и свойства документов, а также возможность создавать и применять сложные контентно-зависимые правила.
- Наличие только базовой лицензии DeviceLock не позволяет использовать функциональность контроля каналов сетевых коммуникаций (протоколов), не позволяет создавать и применять контентно-зависимые правила, используя шаблоны регулярных выражений, ключевые слова и свойства документов, не позволяет создавать и применять сложные контентно-зависимые правила. При этом можно создавать и использовать контентно-зависимые правила на основе определения типа файла (File Type Detection).
- Наличие базовой лицензии DeviceLock и лицензии на модуль ContentLock дает возможность создавать и применять контентно-зависимые правила, используя шаблоны регулярных выражений, ключевые слова и свойства документов, возможность создавать и применять сложные контентно-зависимые правила, а также правила на основе определения типа файла (File Type Detection). При этом невозможно использовать функциональность контроля каналов сетевых коммуникаций (протоколов).
- Наличие базовой лицензии DeviceLock и лицензии на модуль NetworkLock дает возможность использовать функциональность контроля каналов сетевых коммуникаций (протоколов), а также возможность создавать и применять контентно-зависимые правила на основе определения типа файла (File Type Detection). При этом невозможно создавать и применять контентно-зависимые правила, используя шаблоны регулярных выражений, ключевые слова и свойства документов, невозможно создавать и применять сложные контентно-зависимые правила.
- Наличие базовой лицензии DeviceLock обязательно, наличие лицензий на модули ContentLock и NetworkLock не обязательно. Если отсутствует, повреждена или недействительна базовая лицензия DeviceLock, программный комплекс DeviceLock будет работать в режиме пробной эксплуатации. Количество лицензий на модули ContentLock и/или NetworkLock должно быть равным или больше количества базовых лицензий DeviceLock.
- Период пробной эксплуатации для модулей ContentLock и NetworkLock составляет 30 дней.

Модуль мониторинга активности пользователей

DeviceLock DLP содержит дополнительный модуль мониторинга активности пользователей (UAM), расширяющий функциональные возможности комплекса DeviceLock. Этот модуль устанавливается автоматически, но требует отдельной лицензии на использование. Подробнее о лицензии для этого модуля см. в разделе Лицензирование модуля UAM.

Модуль DeviceLock UAM предоставляет возможность мониторинга действий пользователя посредством таких инструментов, как видеозапись экрана пользователя, запись всех нажатий клавиш, информация о процессах и приложениях, которые выполнялись и запускались во время записи. Такие виды мониторинга позволяют существенно расширить доказательную базу при расследовании инцидентов информационной безопасности, а также помогают выявлять подозрительное поведение пользователей и злоупотребления привилегиями доступа или политиками защиты данных, что в результате приводит к снижению рисков утечки данных.

Важной особенностью модуля DeviceLock UAM является возможность записи экрана, нажатия клавиш и информации о процессах при наступлении заданного события. Правила записи в DeviceLock UAM можно задавать на основе таких видов событий, как срабатывание контентно-зависимого правила, подключение внешнего накопителя, наличие в системе определенного процесса и т.д.

Для осуществления мониторинга активности пользователей сервис DeviceLock записывает в видео формате действия, происходящие на экране пользовательского компьютера, а также выполняет запись того, какие клавиши нажимает пользователь на клавиатуре, и сохраняет дополнительные сведения, такие как имя активного приложения, заголовок активного окна и т.д. Имеется возможность сбора данных с пользовательских компьютеров на сервер DeviceLock Enterprise Server, где уполномоченные лица могут просматривать и анализировать записи активности пользователей.

Возможность записи действий пользователя дает ряд преимуществ при обнаружении угроз утечки данных. Сервис DeviceLock записывает в точности то, что пользователь видит на экране компьютера, независимо от используемых приложений и протоколов или уровня привилегий пользователя. Ввод с клавиатуры и другие данные, записанные сервисом DeviceLock вместе с видео, могут быть использованы для отслеживания определенных действий пользователя.

Сервис DeviceLock предусматривает различные критерии запуска, позволяющие начинать запись при наступлении определенных событий или условий. В зависимости от выбранного критерия запись может начинаться, например, при подключении определенного устройства, запуске некоторого приложения или несанкционированной попытке записи файла или передачи сообщения. Критерии запуска позволяют сервису DeviceLock выполнять выборочную запись вызывающих подозрения действий пользователя. Вот несколько примеров имеющихся критериев запуска:

- VPN connection exists (Существует VPN-подключение)
- Wireless connection exists (Существует беспроводное подключение)
- Process “<имя процесса>” exists (Существует процесс “<имя процесса>”)
- Content-Aware rule “<имя правила>” is triggered (Сработало контентно-зависимое правило “<имя правила>”)
- Storage device is attached (Подключено устройство хранения данных)
- Read access to “<имя устройства / протокола>” is denied (Запрещен доступ на чтение к “<имя устройства / протокола>”)
- Write access to “<имя устройства / протокола>” is denied (Запрещен доступ на запись к “имя устройства / протокола”)

Подробнее о критериях запуска записи см. в разделе Настройка критериев запуска главы Мониторинг активности пользователей.

Данные мониторинга активности пользователей первоначально сохраняются на локальном компьютере, что позволяет просматривать локальные записи пользовательских действий в консоли DeviceLock Management Console, подключенной к сервису DeviceLock. Так можно просматривать только записи, выполненные сервисом DeviceLock на локальном компьютере.

Для централизованного просмотра и анализа записей с различных компьютеров необходимо передать данные мониторинга активности пользователей на сервер DeviceLock Enterprise Server. Серверы для сбора и хранения данных задаются соответствующим параметром сервиса DeviceLock. При необходимости данные с разных серверов можно объединить для просмотра и анализа на центральном сервере, используя консолидацию журналов.

Подробнее о средствах просмотра записей мониторинга см. в разделе Просмотр активности пользователей главы Мониторинг активности пользователей.

Лицензирование модуля UAM

Чтобы использовать модуль UAM, необходимо приобрести и установить лицензию DeviceLock UAM в дополнение к основной лицензии DeviceLock. Лицензия UAM определяет максимально допустимое количество компьютеров, на которых можно использовать сервис DeviceLock для мониторинга активности пользователей.

Установите лицензию UAM на компьютер с консолью DeviceLock Management Console, чтобы управлять мониторингом активности пользователей на компьютерах с сервисом DeviceLock:

- Просматривать и изменять параметры мониторинга активности пользователей.
- Настраивать, просматривать и изменять правила записи мониторинга активности пользователей.
- Просматривать записи мониторинга активности пользователей на сервисе DeviceLock.

Для применения серверных политик и задач мониторинга компьютеров, в которых заданы параметры и правила мониторинга активности пользователей, на сервере DeviceLock Enterprise Server должна быть установлена лицензия мониторинга активности пользователей. Количество компьютеров, к которым применяются такие политики и задачи, не может быть больше указанного в этой лицензии.

Для сбора данных мониторинга активности пользователей на сервере DeviceLock Enterprise Server должна быть установлена основная лицензия DeviceLock. Количество компьютеров, с которых сервер собирает данные мониторинга активности пользователей, не может быть больше указанного в этой лицензии.

При планировании лицензии UAM учитывайте следующее:

- Модуль UAM невозможно использовать без основной лицензии DeviceLock. Основная лицензия должна быть установлена на компьютере с консолью DeviceLock Management Console, иначе DeviceLock работает в пробном режиме не более 30 дней.
- Указанное в лицензии UAM количество компьютеров должно быть равно количеству компьютеров, указанному в основной лицензии, иначе модуль UAM работает в пробном режиме не более 30 дней.
- Лицензия UAM является необязательной и влияет только на модуль UAM. Другие модули и функции DeviceLock при правильном лицензировании доступны независимо от того, установлена ли лицензия UAM.

Правила обеспечения безопасности

Ниже приведен ряд основополагающих правил обеспечения безопасности, которые должны соблюдаться для компьютеров, подключаемых к корпоративной сети:

- **Измените последовательность загрузки.** Жесткий диск должен быть первым загрузочным устройством. Измените последовательность загрузки в BIOS таким образом, чтобы компьютер не мог загружаться с дискеты, USB-устройства или DVD/CD-ROM. Если жесткий диск не является первым загрузочным устройством, кто угодно сможет использовать загрузочный CD или флеш-диск, подключаемый к USB, чтобы получить доступ к жесткому диску.
- **Защитите BIOS паролем.** Пароль должен быть установлен для доступа к BIOS, чтобы только человек, знающий его, мог вносить изменения в конфигурацию. Если BIOS не защищен паролем, кто угодно может изменить последовательность загрузки и использовать загрузочный CD, дискету или флеш-диск (см. выше).
- **Опечатайте корпусы компьютеров и шасси.** Опечатайте аппаратные компоненты. Существует возможность подключить внешнее загрузочное устройство непосредственно к компьютеру и получить доступ к жесткому диску. Более того, если кто-то получит физический доступ к материнской плате, ему будет очень просто найти переключатель очистки CMOS и затем стереть пароль для доступа к BIOS (см. выше).
- **Не предоставляйте права администратора обычному пользователю.** Рядовые пользователи не должны входить в локальную группу Администраторы. Также не следует давать им административные права на рабочие компьютеры.

  Однако даже если пользователи вашей сети имеют административные привилегии на локальных компьютерах, DeviceLock способен обеспечить необходимый уровень защиты. Никто, за исключением авторизированного администратора программы DeviceLock, не может подключиться, остановить или удалить сервис DeviceLock. Даже члены локальной группы Администраторы не могут отключить DeviceLock, если они не являются администраторами DeviceLock.
- **Удалите среду/консоль восстановления Windows.** Используя среду восстановления Windows на локальном компьютере, кто угодно может загрузить компьютер в режиме восстановления системы и отключить сервис DeviceLock (тем не менее, для этого потребуется пароль локального администратора). Поэтому рекомендуется не допускать использования среды восстановления Windows обычными пользователями. Параметры восстановления системы описаны в статье Microsoft по адресу support.microsoft.com/ru-ru/kb/307654. Сведения о среде восстановления Windows см. в статье Microsoft по адресу msdn.microsoft.com/ru-ru/dn938364.

2

Установка DeviceLock

В этой главе:

Системные требования

Развертывание сервиса DeviceLock для Windows

Развертывание сервиса DeviceLock для Mac

Установка консолей управления

Установка DeviceLock Enterprise Server

Установка DeviceLock Content Security Server

Системные требования

В состав программного комплекса DeviceLock DLP входят сервис DeviceLock, сервер DeviceLock Enterprise Server, сервер DeviceLock Content Security Server, а также консоли управления DeviceLock Management Console, DeviceLock Group Policy Manager и DeviceLock Enterprise Manager. Ниже приводятся системные требования по каждому из этих компонентов.

Компьютер для установки сервиса DeviceLock должен отвечать следующим требованиям:

Операционная система для сервиса DeviceLock для Windows	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 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.
Операционная система для сервиса DeviceLock для Mac	macOS 10.15 (Catalina) или macOS 11.2.3 (Big Sur).
Память (ОЗУ)	Минимум: 512 МБ
Свободное место на жестком диске	Минимум: 400 МБ
Процессор	Минимум: Intel Pentium 4
Поддерживаемые средства виртуализации	Microsoft Remote Desktop Services, Citrix XenDesktop / XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox и Windows Virtual PC.

Примечание: Запись активности пользователей может выполняться только на компьютерах под управлением Windows 7 / Windows Server 2008 R2 или более поздней версии Windows.

Компьютер для установки консолей управления должен отвечать следующим требованиям:

Операционная система	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 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.
Память (ОЗУ)	Минимум: 512 МБ

Свободное место на жестком диске	Минимум: 1 ГБ
Процессор	Минимум: Intel Pentium 4

Примечание:

- Для просмотра графов связей, работы с поисковым сервером, управления цифровыми отпечатками, а также для работы с журналом активности пользователей и просмотра отчетов сервера Discovery требуется Internet Explorer 9 или более поздней версии.
- Для просмотра пользовательских досье требуется Internet Explorer 11 или более поздней версии.
- Просматривать записи журнала активности пользователей можно только в консоли, установленной на компьютере под управлением Windows 7 / Windows Server 2008 R2 или более поздней версии Windows.

  Для просмотра видеозаписей активности пользователей в консоли на Windows Server должен быть установлен компонент Возможности рабочего стола (Desktop Experience) / База мультимедиа (Media Foundation).

  Для просмотра видеозаписей активности пользователей в консоли на выпусках Windows N или KN необходимо установить пакет Media Feature Pack. Инструкции по установке см. в support.microsoft.com/help/3145500.

Системные требования для сервера DeviceLock Enterprise Server:

Операционная система	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.
Память (ОЗУ)	Минимум: 1 ГБ Рекомендуется: 8 ГБ
Свободное место на жестком диске	Минимум: 1 ГБ Рекомендуется: 800 ГБ (в случае локального сервера базы данных)
Процессор	Минимум: Intel Pentium 4 Рекомендуется: 2x Intel Xeon Quad Core 2.33 ГГц
Сервер базы данных	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017 или 2019, любой выпуск, в том числе SQL Server Express. - или - PostgreSQL версии 9.5 (9.5.19 или выше), 9.6 (9.6.15 или выше), 10 (10.10 или выше), 11 (11.5 или выше) или 12 (12.0 или выше). PostgreSQL ODBC Driver версии 9.6.500 или выше. Предпочтительной является самая последняя версия драйвера.

Внимание: При использовании PostgreSQL в качестве сервера базы данных DeviceLock Enterprise Server обеспечивает сбор и администрирование следующих журналов: аудита, теневого копирования, удаленных данных теневого копирования, журнала сервера, а также консолидацию этих журналов. Другие функции сервера DeviceLock Enterprise Server в этом случае недоступны.

Системные требования для сервера DeviceLock Content Security Server:

Операционная система	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.
Память (ОЗУ)	Минимум: 1 ГБ Рекомендуется: 8 ГБ
Свободное место на жестком диске	Минимум: 1 ГБ Рекомендуется: 800 ГБ (в случае локального сервера базы данных)
Процессор	Минимум: Intel Pentium 4 Рекомендуется: 2x Intel Xeon Quad Core 2.33 ГГц
Сервер базы данных	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017 или 2019, любой выпуск, в том числе SQL Server Express.

Для установки и настройки DeviceLock на автономном компьютере требуются права локального администратора. Для установки и настройки DeviceLock в домене Active Directory требуются права администратора домена.

Для использования DeviceLock в локальной сети требуется сетевой протокол TCP/IP. Однако DeviceLock может работать и на компьютерах без подключения к локальной сети. Подключение к сети необходимо для дистанционного доступа к сервису DeviceLock на разных компьютерах.

Следующие TCP/UDP-порты должны быть открыты для сетевой связи и обмена данными между различными компонентами DeviceLock:

- 135 (TCP) - Порт службы удаленного вызова процедур (Remote Procedure Call, RPC).
- 137 (UDP) - Порт службы имен NetBIOS (Name Resolution).
- 138 (UDP) - Порт службы датаграмм NetBIOS (Datagram Service).
- 139 (TCP) - Порт службы сессий NetBIOS (Session Service).
- 445 (TCP) - Порт протокола блока сообщений сервера (Server Message Block, SMB). Используется консолью DeviceLock Management Console при управлении сервисом DeviceLock на удаленных компьютерах.
- 9132 (TCP) - Порт сервиса DeviceLock по умолчанию.
- 9133 (TCP) - Порт сервера DeviceLock Enterprise Server по умолчанию. Этот порт по умолчанию используется также для консолидации журналов и должен быть открыт как на центральном сервере, так и на удаленных серверах консолидации.
- 9134 (TCP) - Порт сервера DeviceLock Content Security Server по умолчанию.

Также необходимо установить тип запуска “Автоматический” для следующих служб:

- Удалённый реестр (Remote Registry)
- Удалённый вызов процедур (Remote Procedure Call, RPC)
- Служба базовой фильтрации (Base Filtering Engine)

Примечание: Устанавливать типа запуска для службы базовой фильтрации требуется только на Windows 8 или более поздних версиях Windows.

Дополнительные системные требования для агентов Discovery

Сервер Discovery, входящий в состав DeviceLock Content Security Server, может устанавливать и использовать агент DeviceLock Discovery на клиентских компьютерах. Для установки агента DeviceLock Discovery компьютер должен отвечать следующим требованиям:

Операционная система	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 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.
Память (ОЗУ)	Минимум: 512 MB
Свободное место на жестком диске	Минимум: 200 MB
Процессор	Минимум: Intel Pentium 4

Следующие TCP/UDP-порты должны быть открыты, чтобы обеспечить сетевую связь агента Discovery с другими компонентами DeviceLock, а также сканирование SMB-ресурсов:

- 135 (TCP) - Порт службы удаленного вызова процедур (Remote Procedure Call, RPC).
- 137 (UDP) - Порт службы имен NetBIOS (Name Resolution).
- 138 (UDP) - Порт службы датаграмм NetBIOS (Datagram Service).
- 139 (TCP) - Порт службы сессий NetBIOS (Session Service).
- 9135 (TCP) - Порт агента Discovery по умолчанию.
- 445 (TCP) - Порт протокола блока сообщений сервера (Server Message Block, SMB). Используется при сканировании SMB-ресурсов на удаленных компьютерах.

Развертывание сервиса DeviceLock для Windows

Сервис DeviceLock должен быть установлен на каждом компьютере, где требуется контролировать доступ пользователей к устройствам и сетевым протоколам. Предусмотрено несколько способов установки сервиса DeviceLock на компьютеры пользователей:

- Интерактивная установка
- Установка без вмешательства пользователя
- Установка с помощью Systems Management Server
- Установка в DeviceLock Management Console
- Установка в DeviceLock Enterprise Manager
- Установка через групповые политики
- Установка с помощью DeviceLock Enterprise Server

Рекомендации

В силу специфики действий сервиса DeviceLock антивирусы могут принимать исполняемые файлы DeviceLock за вредоносное ПО и выполнять внеплановое сканирование его служебных каталогов. Это может вызывать заметное снижение производительности сервиса DeviceLock и самого компьютера, а также приводить к другим проблемам.

Чтобы предотвратить потерю производительности компьютера с установленным сервисом DeviceLock, желательно добавить следующие папки в список исключений для антивируса:

1. Папка установки DeviceLock - По умолчанию `%ProgramFiles%\DeviceLock` или `%ProgramFiles(x86)%\DeviceLock` в 32-разрядной или 64-разрядной системе, соответственно.
2. Папка теневого копирования DeviceLock - По умолчанию `%SystemRoot%\SHADOW`, может быть изменены настройкой параметра Локальная директория.

Интерактивная установка

Запустите программу установки `setup.exe` и следуйте инструкциям на страницах мастера установки.

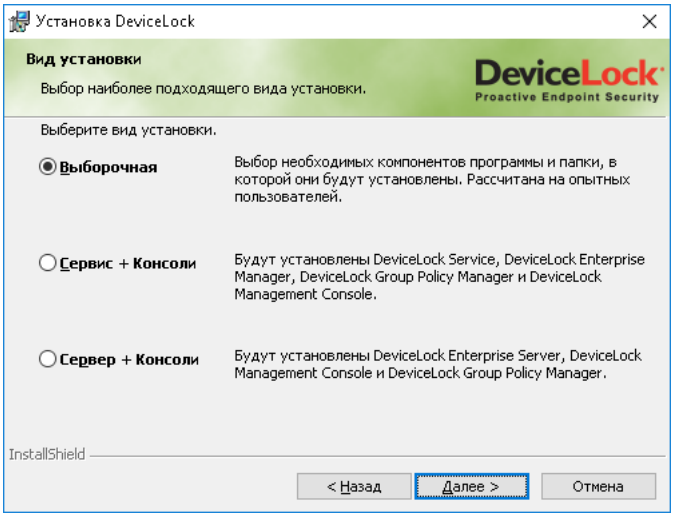
Примечание:

- Необходимо запускать `setup.exe` на каждом компьютере, где должен быть установлен сервис DeviceLock.
- Если вы устанавливаете сервис DeviceLock поверх уже существующей предыдущей версии, убедитесь, что у вас есть административные права доступа к сервису DeviceLock, в противном случае вы не сможете продолжить установку.

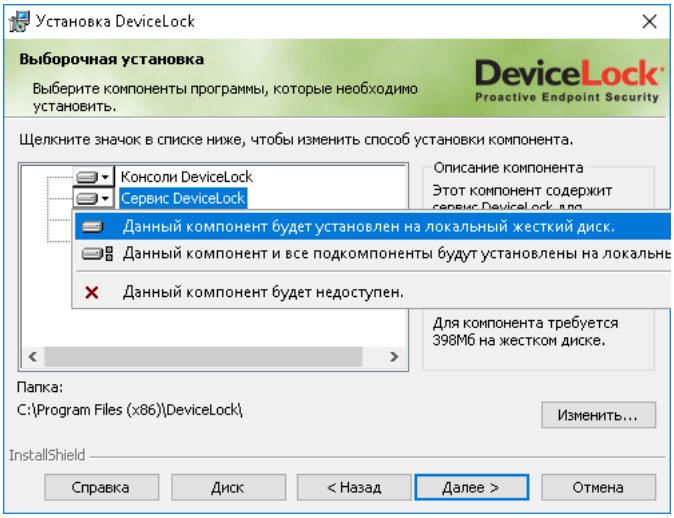
На странице **Лицензионное соглашение** ознакомьтесь с лицензионным соглашением и выберите опцию **Я принимаю условия лицензионного соглашения**, чтобы принять условия лицензионного соглашения и продолжить установку.

На странице **Сведения о пользователе** введите свое имя и название организации.

На странице **Вид установки** выберите требуемый тип установки.



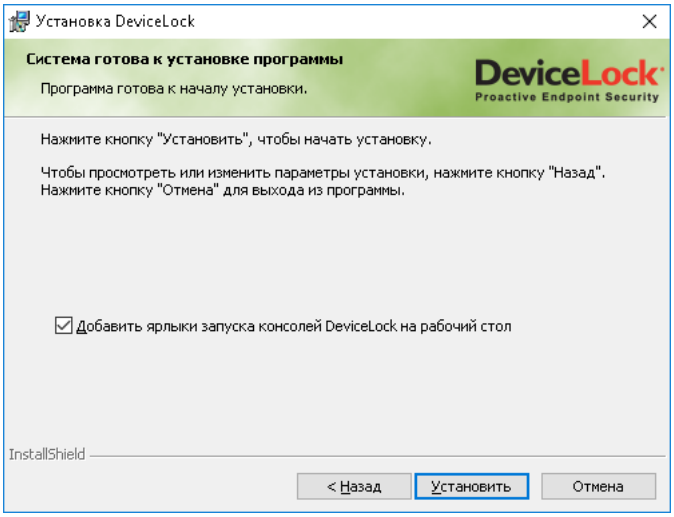
Можно установить сервис DeviceLock и консоли управления DeviceLock, выбрав опцию **Сервис + Консоли** или установить только сервис DeviceLock, выбрав опцию **Выборочная** и потом отметив компонент **Сервис DeviceLock**.



Примечание: На странице **Выборочная установка** можно также выбрать для установки компонент RSoP. Этот компонент обеспечивает поддержку режима планирования результирующей политики (RSoP) DeviceLock на контроллерах домена. Компонент RSoP необходим только тогда, когда на компьютере установлены консоли управления DeviceLock, но не установлен сервис DeviceLock. Описание режима планирования RSoP можно найти в документации Microsoft по адресу technet.microsoft.com/library/cc758010.aspx.

На странице **Выборочная установка** можно изменить папку установки. Для этого нажмите кнопку **Изменить** и выберите папку в появившемся диалоговом окне. Папка установки по умолчанию: `%ProgramFiles%\DeviceLock`.

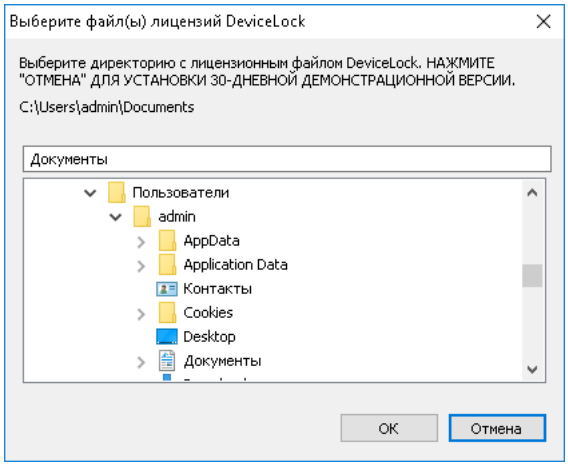
На странице **Система готова к установке программы** нажмите кнопку **Установить**, чтобы начать установку. Установите флажок **Добавить ярлыки запуска консолей DeviceLock на рабочий стол**, чтобы добавить ярлыки запуска консолей DeviceLock Management Console (оснастка MMC), DeviceLock Enterprise Manager и DeviceLock Service Settings Editor на рабочий стол.



Если выбрана установка консолей управления DeviceLock, программа установки может предложить создание сертификата DeviceLock. Появится следующее сообщение: “Вы хотите создать новый сертификат DeviceLock (открытый и секретный ключи)? Нажмите “Нет”, если у Вас уже есть сертификат DeviceLock и не нужно создавать новую пару ключей.”

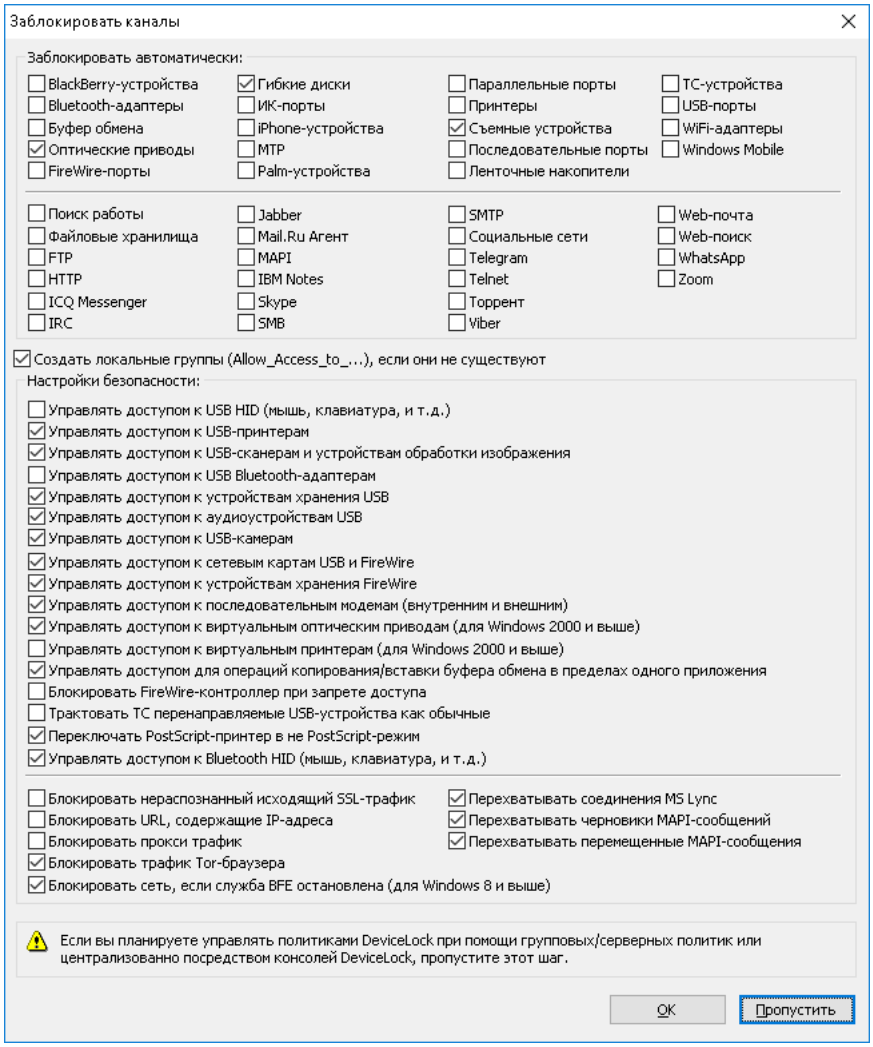
Сертификаты можно создавать с помощью мастера создания сертификата (см. Сертификаты DeviceLock далее в этом документе). Этот мастер устанавливается вместе с консолями управления DeviceLock. Поэтому, если нет уверенности, нужен ли новый сертификат, нажмите кнопку **Нет** и продолжайте установку.

Если была выбрана опцию **Сервис + Консоли**, программа установки может запросить файлы лицензий DeviceLock. При отсутствии этих файлов нажмите кнопку **Отмена**, чтобы установить DeviceLock в ознакомительном 30-дневном режиме.



Подробнее о лицензиях DeviceLock см. в разделе Активация клиентских лицензий.

В процессе установки предоставляется возможность задать разрешения для локальных устройств и протоколов.



Отметьте устройства и/или протоколы, для которых требуется установить разрешения. Отметьте **Создать локальные группы (Allow_Access_to_...), если они не существуют**, и программа создаст специальные локальные группы пользователей Allow_Access_To_ для каждого типа каналов (например, Allow_Access_To_Floppy для дисководов), если они не существовали на локальном компьютере.

Программа назначит права **Чтение**, **Запись**, **Форматирование** и **Извлечение** членам группы Администраторы и локальной учетной записи системы. Члены группы Allow_Access_To_ будут иметь права **Чтение**, **Запись**, и **Извлечение**.

Также имеется возможность определить дополнительные настройки безопасности, позволяющие разрешить или запретить сервису DeviceLock контролировать доступ к устройствам определенного типа (см. раздел Настройки безопасности (обычный профиль)).

Установите флажки **Управлять доступом к USB HID (мышь, клавиатура, и т.д.)**, **Управлять доступом к USB-принтерам**, **Управлять доступом к USB-сканерам и устройствам обработки изображения**, **Управлять доступом к USB Bluetooth-адаптерам**, **Управлять доступом к устройствам хранения USB** и **Управлять доступом к устройствам хранения FireWire**, чтобы разрешить сервису DeviceLock контролировать доступ к устройствам ввода (мышь, клавиатура и т.д.), принтерам, сканерам и фотоаппаратам, Bluetooth-адаптерам или устройствам хранения информации (таким как флеш-диски), подключаемым к портам USB и FireWire. Чтобы разрешить контроль доступа к веб-камерам

и/или аудиоустройствам, подключаемым к порту USB, установите флажок **Управлять доступом к USB-камерам** и/или **Управлять доступом к аудиоустройствам USB**. Чтобы разрешить контроль доступа для USB и FireWire-сетевых карт, установите флажок **Управлять доступом к сетевым картам USB и FireWire**. В противном случае, даже если порты (USB и/или FireWire) заблокированы, перечисленные выше устройства, подключенные к этим портам, будут продолжать работать как обычно. Чтобы разрешить контроль доступа для модемов (внутренних или внешних), установите флажок **Управлять доступом к последовательным модемам (внутренним и внешним)**. Чтобы отключить блокирование виртуальных дисководов CD/DVD/BD, снимите флажок **Управлять доступом к виртуальным оптическим приводам**. Чтобы отключить блокирование виртуальных принтеров, снимите флажок с **Управлять доступом к виртуальным принтерам**. Чтобы разрешить контроль доступа для операций копирования/вставки в/из буфера обмена в пределах приложения, установите флажок **Управлять доступом для операций копирования/вставки буфера обмена в пределах одного приложения**. В противном случае, даже если заблокирован буфер обмена, контроль доступа для операций копирования/вставки в пределах одного приложения приложениями будет отключен. Чтобы отключить FireWire-контроллер при наличии у учетной записи Everyone разрешения "Нет доступа" для типа FireWire port, установите флажок **Блокировать FireWire-контроллер при запрете доступа**. Чтобы разрешить контролировать доступ к Bluetooth-устройствам ввода (мышь, клавиатура и т.д.), установите флажок **Управлять доступом к Bluetooth HID (мышь, клавиатура, и т.д.)**.

Установите флажок **Переключать PostScript-принтер в не PostScript-режим**, чтобы принтеры PostScript могли работать как обычные принтеры. Это позволяет решить проблему, из-за которой сервис DeviceLock не может корректно выполнить теневое копирование и анализ данных для печати на принтерах, использующих драйвер PostScript.

Установите флажок **Трактовать TC перенаправляемые USB-устройства как обычные**, чтобы сервис DeviceLock мог управлять доступом ко всем USB-устройствам, перенаправленным в терминальную сессию Citrix XenDesktop/MS RemoteFX в соответствии с правами, заданными для типа USB-порт. В противном случае, сервис DeviceLock будет управлять доступом ко всем USB-устройствам, перенаправленным в терминальную сессию Citrix XenDesktop/MS RemoteFX, в соответствии с набором прав **Доступ к USB-устройствам** для типа **TC-устройства**.

Также можно задать настройки безопасности для протоколов (см. раздел Настройки безопасности для протоколов).

Чтобы сервис DeviceLock мог выполнять аудит и блокирование нераспознанного трафика SSL, установите флажок **Блокировать нераспознанный исходящий SSL-трафик**. Если эта настройка отключена, то даже при заблокированных протоколах нераспознанный исходящий SSL-трафик не блокируется и аудит для него не выполняется.

Чтобы сервис DeviceLock мог блокировать все URL, содержащие IP-адреса, для пользователей, которым разрешен доступ по протоколу HTTP, установите флажок **Блокировать URL, содержащие IP-адреса**. Эта настройка блокирует, в частности, доступ к веб-сайтам по IP-адресу.

Чтобы сервис DeviceLock мог выполнять аудит и блокирование трафика от прокси-серверов, установите флажок **Блокировать прокси трафик**. Поддерживаются следующие типы прокси-серверов: HTTP, SOCKS4 и SOCKS5.

Чтобы сервис DeviceLock мог блокировать подключение к сети Tor, предотвращая использование Tor-браузера, установите флажок **Блокировать трафик Tor-браузера**.

Чтобы сервис DeviceLock мог блокировать весь сетевой трафик при остановленной системной службе базовой фильтрации (Base Filtering Engine), установите флажок **Блокировать сеть, если служба BFE остановлена (для Windows 8 и выше)**.

Чтобы сервис DeviceLock мог перехватывать сетевой трафик приложения Microsoft Lync 2010 или Microsoft Office Communicator, установите флажок **Перехватывать соединения MS Lync**.

Чтобы сервис DeviceLock мог контролировать черновики сообщений, которые сохраняются приложением Outlook в папке черновиков на сервере Exchange, установите флажок **Перехватывать черновики MAPI-сообщений**.

Чтобы сервис DeviceLock мог контролировать сообщения, которые Outlook импортирует на сервер Exchange из внешних файлов почтовых сообщений (.msg-файлов) или других (внешних) почтовых ящиков, установите флажок **Перехватывать перемещенные MAPI-сообщения**.

Нажмите кнопку **OK**, чтобы применить настройки к устанавливаемому сервису DeviceLock. Для установки сервиса DeviceLock без применения этих настроек нажмите кнопку **Пропустить**. Просмотреть или изменить настройки можно будет с помощью консоли управления DeviceLock.

Далее, на странице **Мастер установки завершен** нажмите кнопку **Готово**, чтобы завершить процесс установки. С завершающей страницы мастера установки можно перейти на веб-сайт DeviceLock. Этот вариант выбран по умолчанию.

Примечание: Удалить DeviceLock можно следующим образом:

- Используйте средство **Программы и компоненты** панели управления Windows (**Установка и удаление программ** на ранних версиях Windows).

  - или -
- Выберите пункт **Удалить DeviceLock** в меню **Пуск** Windows.

Установка без вмешательства пользователя

DeviceLock позволяет выполнить установку без вмешательства пользователя. Для этого нужно создать пакетный файл, который выполнит все необходимые действия. Чтобы установить сервис DeviceLock без участия пользователя, запустите файл `setup.exe` с ключом `/s` (например, `c:\setup.exe /s`). Параметры установки можно задать в конфигурационном файле `devicelock.ini`. Этот файл должен находиться той же папке, что и файл `setup.exe`.

Файл `devicelock.ini` можно править в любом текстовом редакторе (например, в приложении Блокнот). Удалите точку с запятой (;) перед параметром, чтобы присвоить новое значение этому параметру, либо оставьте точку с запятой, чтобы присвоить значение по умолчанию.

В файле `devicelock.ini` имеются два раздела (`[Install]` и `[Misc]`), каждый со своим набором параметров. Эти параметры описаны ниже.

Раздел `[Install]`

Чтобы установить сервис DeviceLock, установите параметр `Service` в единицу:

```
Service = 1
```

Аналогичным образом можно установить консоли управления DeviceLock и документацию, используя параметры `Manager` и `Documents`.

Если требуется только обновить сервис DeviceLock без изменения существующих настроек, используйте параметр `OnlyUpgradeService`:

```
OnlyUpgradeService = 1
```

В этом случае программа установки игнорирует все заданные параметры и только обновляет сервис DeviceLock.

Можно задать путь к папке, в которую будет установлен DeviceLock:

```
InstallDir = C:\Program Files\DeviceLock
```

Программа использует этот параметр, если не может найти существующую установку DeviceLock на данном компьютере.

При наличии файлов лицензии для DeviceLock можно указать их местоположение:

```
RegFileDir = C:\Directory
```

где `C:\Directory` - папка, в которой находятся файлы лицензии.

Лицензии можно не указывать, если устанавливается только сервис DeviceLock. Лицензии требуются для консолей управления DeviceLock и модулей ContentLock и NetworkLock.

Чтобы указать TCP-порт для сервиса DeviceLock, задайте значение параметра `FixedPort`:

```
FixedPort = [номер порта]
```

где `номер порта` - это номер TCP-порта для доступа консоли управления к сервису DeviceLock. Чтобы использовать автоматический выбор порта, укажите номер порта `0`. По умолчанию сервис DeviceLock использует порт `9132`.

Если параметр `CreateGroups` установлен в `1`, программа установки создаст специальную локальную группу пользователей Allow_Access_To_ для каждого типа устройств (например, Allow_Access_To_Floppy для гибких дисков) при отсутствии такой группы на локальном компьютере.

Чтобы задать настройки, разрешения, а также правила аудита и оповещения для сервиса DeviceLock, в параметре `SettingsFile` укажите полный путь к файлу настроек:

```
SettingsFile = C:\settings.dls
```

Файл настроек может быть создан с помощью консолей DeviceLock Management Console, DeviceLock Group Policy Manager и/или DeviceLock Service Settings Editor.

Раздел `[Misc]`

Если требуется запустить какую-либо программу после успешной установки DeviceLock, задайте параметр `Run`:

```
Run = C:\mybatchfile.bat
```

Для запрета автоматической перезагрузки компьютера после завершения установки, даже если программа установки требует этого, установите параметр `DisableRestart` в `1`.

Установка с помощью Systems Management Server

Используя автоматическую установку (см. Установка без вмешательства пользователя), можно также выполнить развертывание сервиса DeviceLock на компьютерах в локальной сети при помощи Microsoft Systems Management Server (SMS). Используйте файлы `DevLock.pdf` для SMS версии 1.x и `DevLock.sms` для SMS версий 2.0 и выше. Эти файлы входят в состав поставки DeviceLock и находятся в файле `sms.zip`.

Установка в DeviceLock Management Console

Консоль DeviceLock Management Console позволяет выполнить дистанционную установку сервиса DeviceLock.

Примечание: Дистанционная установка сервиса DeviceLock на компьютеры под управлением ОС Windows Vista и более поздних версий возможна только с использованием встроенной учетной записи локального администратора. В доменах Active Directory только члены группы “Администраторы домена” могут выполнять дистанционную установку сервиса DeviceLock. Права администратора также требуются для подключения к сервису DeviceLock посредством консоли DeviceLock Management Console. Дополнительную информацию см. в статье Microsoft по адресу support.microsoft.com/kb/951016.

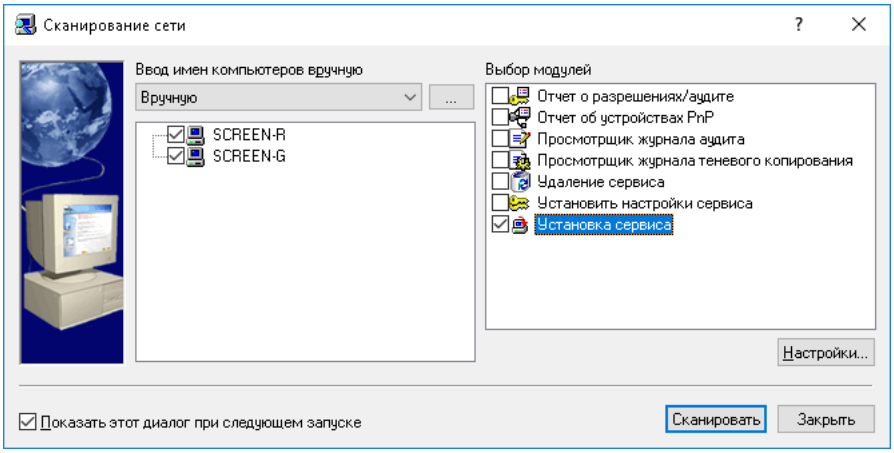
При попытке подключиться к компьютеру, на котором сервис DeviceLock не установлен либо установлена старая версия, консоль управления предложит соответственно установить либо обновить сервис DeviceLock на этом компьютере. Появится следующее сообщение: “Device Lock сервис не установлен на <имя компьютера>. Установить сервис?”

Выберите папку, содержащую файлы, необходимые для установки (файлы `DeviceLock Service.msi`, `DeviceLock Service x64.msi`, `DLRemoteInstaller.exe` и `InstMsiW.exe`). Эти файлы находятся в папке установки DeviceLock (по умолчанию `%ProgramFiles%\DeviceLock`).

По умолчанию установочные файлы сервиса DeviceLock будут скопированы в папку `%ProgramFiles%\DeviceLock Agent`, если сервис DeviceLock еще не был установлен на данном компьютере. Если сервис DeviceLock уже был установлен, но его версия ниже 7.0, консоль управления также скопирует установочные файлы в папку `%ProgramFiles%\DeviceLock Agent`. Если сервис DeviceLock уже был установлен и его версия 7.0 или выше, консоль управления скопирует установочные файлы в папку с существующей версией и старые файлы будут перезаписаны новыми.

Установка в DeviceLock Enterprise Manager

DeviceLock Enterprise Manager предоставляет модуль **Установка сервиса**, позволяющий дистанционно устанавливать сервис DeviceLock на компьютеры в локальной сети.

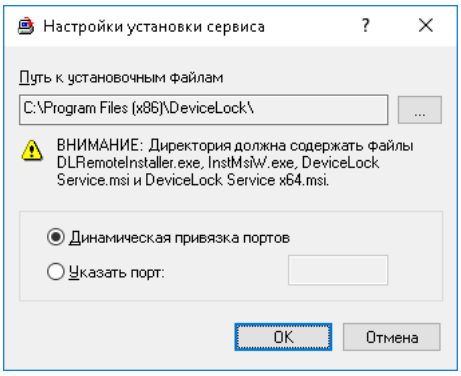


Примечание: Дистанционная установка сервиса DeviceLock на компьютеры под управлением ОС Windows Vista и более поздних версий возможна только с использованием встроенной учетной записи локального администратора. В доменах Active Directory только члены группы “Администраторы домена” могут выполнять дистанционную установку сервиса DeviceLock. Права администратора также требуются для подключения к сервису DeviceLock посредством консоли DeviceLock Management Console. Дополнительную информацию см. в статье Microsoft по адресу support.microsoft.com/kb/951016.

Вначале выберите компьютеры, на которые требуется установить сервис DeviceLock. DeviceLock Enterprise Manager позволяет выбирать компьютеры по типам и именам. Можно также задать список компьютеров вручную, загрузить его из внешнего файла или выбрать компьютеры из LDAP-совместимой службы каталогов (Active Directory, Novell eDirectory, OpenLDAP и т.п.).

Затем выберите модуль **Установка сервиса** и нажмите кнопку **Настройки**, чтобы указать папку с файлами для установки сервиса DeviceLock (файлы `DeviceLock Service.msi`, `DeviceLock Service x64.msi`, `DLRemoteInstaller.exe` и `InstMsiW.exe`). Эти файлы можно найти в папке установки DeviceLock (по умолчанию `%ProgramFiles%\DeviceLock`). Можно также задать TCP-порт для связи сервиса с консолями управления. Чтобы задать

фиксированный порт, выберите опцию **Указать порт**. Для автоматического выбора порта служит опция **Динамическая привязка портов**. По умолчанию сервис DeviceLock использует порт 9132.



По умолчанию установочные файлы сервиса DeviceLock будут скопированы в папку `%ProgramFiles%\DeviceLock Agent`, если сервис DeviceLock не был установлен на данном компьютере. Если сервис DeviceLock уже был установлен, но его версия ниже 7.0, модуль **Install service** также скопирует установочные файлы в папку `%ProgramFiles%\DeviceLock Agent`. Если сервис DeviceLock уже был установлен и его версия 7.0 или выше, модуль **Установка сервиса** скопирует установочные файлы в папку с существующей версией и старые файлы будут перезаписаны новыми.

Установка через групповые политики

Приведенная здесь пошаговая инструкция показывает, как можно выполнить автоматическую установку сервиса DeviceLock при помощи групповой политики в домене Active Directory. Для этого используется MSI-пакет `DeviceLock Service.msi` или `DeviceLock Service x64.msi`.

Примечание: Если групповая политика используется для установки сервиса с настройками из пользовательского MSI-пакета, то настройки, заданные в этом пакете, не применяются в любой из следующих ситуаций:

- На удаленном компьютере, где выполняется установка, у сервиса DeviceLock выключена безопасность по умолчанию.
- В объекте групповой политики, применяемом к этому компьютеру, для сервиса DeviceLock включен параметр **Подавлять локальную политику**.

Инструкции по созданию пользовательского MSI-пакета см. в описании команды Создать MSI-пакет.

Для установки сервиса DeviceLock при помощи групповой политики требуется выполнить следующие действия:

- **Создание точки распространения**

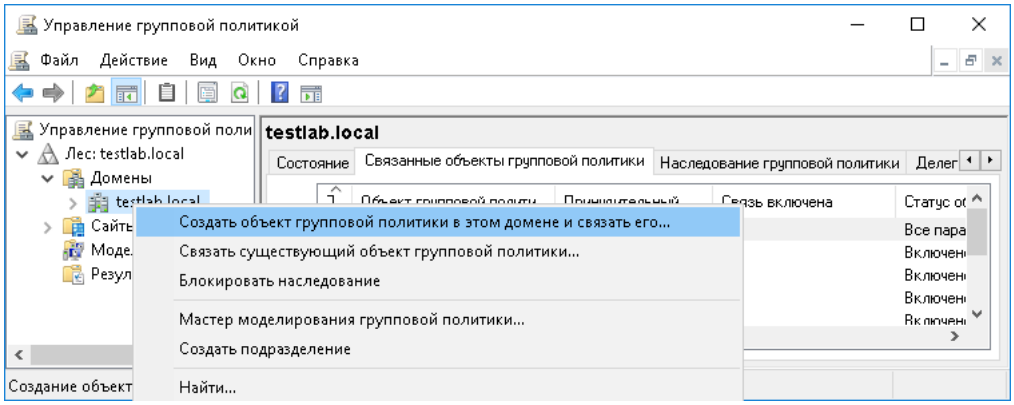
  Чтобы установить сервис DeviceLock, следует создать точку распространения на сервере:

  1. Войти на сервер в качестве администратора.
  2. Создать общедоступную сетевую папку.
  3. Установить права на данную папку, разрешающие доступ к дистрибутиву.
  4. Скопировать установочный пакет `DeviceLock Service.msi` и/или `DeviceLock Service x64.msi` в эту папку.

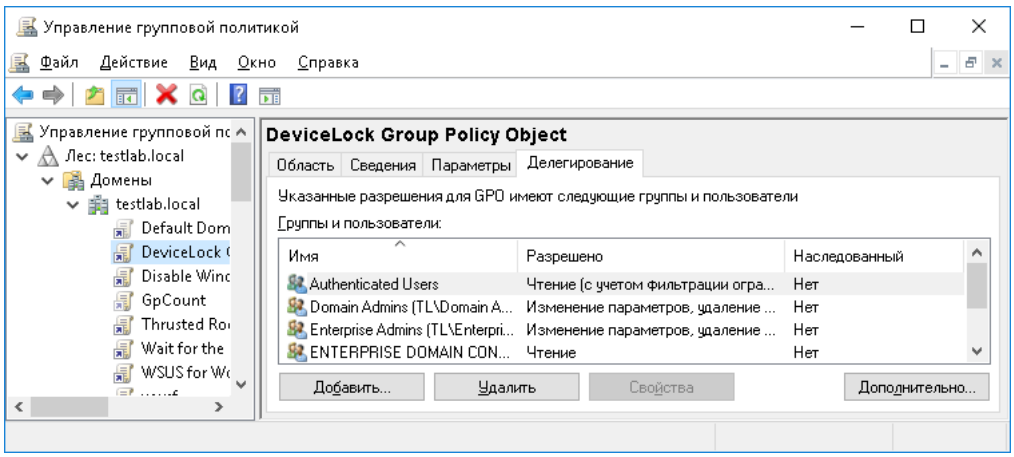
- **Создание объекта групповой политики**

  Чтобы создать объект групповой политики (GPO), с помощью которого будет устанавливаться сервис DeviceLock:

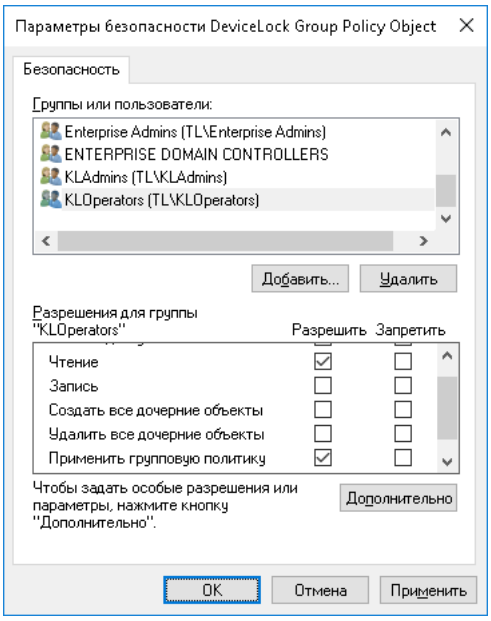
  1. В дереве консоли “Управление групповой политикой” щелкните правой кнопкой мыши домен Active Directory и выберите в контекстном меню команду **Создать объект групповой политики в этом домене и связать его**.



  2. Введите имя для этого объекта и нажмите клавишу ENTER.
  3. Выберите объект групповой политики в дереве консоли, щелкните вкладку **Делегирование** и затем нажмите кнопку **Дополнительно**.



4. В появившемся диалоговом окне **Параметры безопасности** установите флажок **Запретить**, соответствующий праву **Применить групповую политику**, для тех групп, для которых требуется запретить применение данной политики. Установите флажок **Разрешить** для тех групп, к которым будет применяться данная политика.

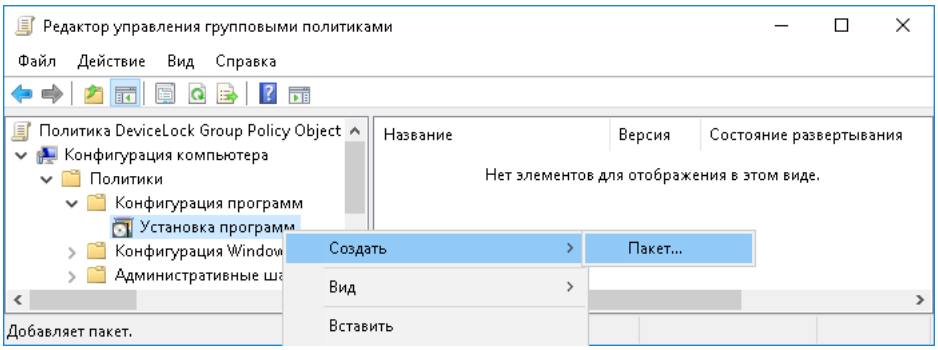


5. После завершения нажмите **OK**.

- **Установка пакета**

  Для установки сервиса DeviceLock на компьютеры под управлением Windows:

  1. Используйте консоль “Управление групповой политикой”, чтобы открыть объект групповой политики в редакторе управления групповыми политиками.
  2. В разделе **Конфигурация компьютера** раскройте пункт **Конфигурация программ**.
  3. Нажмите правой кнопкой мыши элемент **Установка программ**, выберите **Создать** и затем щелкните **Пакет**.

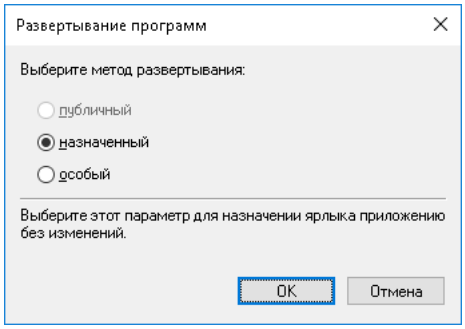


  4. В диалоге **Открытие** введите полный сетевой путь (UNC) к общей сетевой папке, содержащей MSI-пакет. Пример: `\\file server\share\DeviceLock Service.msi`.

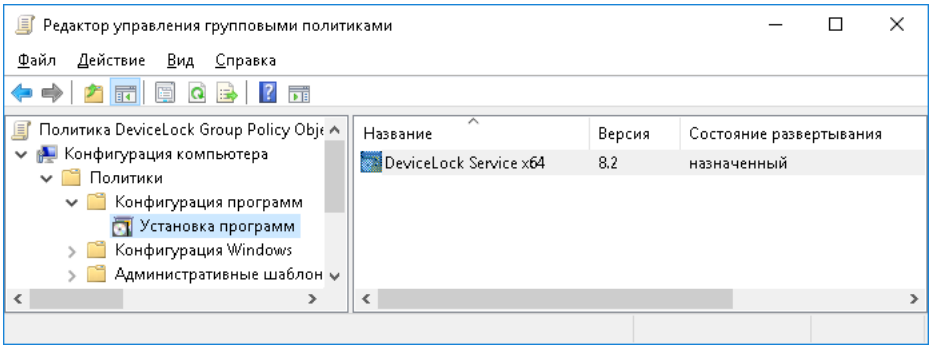
     Внимание: Не пытайтесь указать местоположение в Проводнике. Убедитесь, что путь к общей папке указан в формате UNC.

  5. Нажмите **Открыть**.

6. Выберите опцию **Назначенный**, а затем нажмите **OK**.



Пакет будет добавлен в правую часть окна редактора управления групповыми политиками.

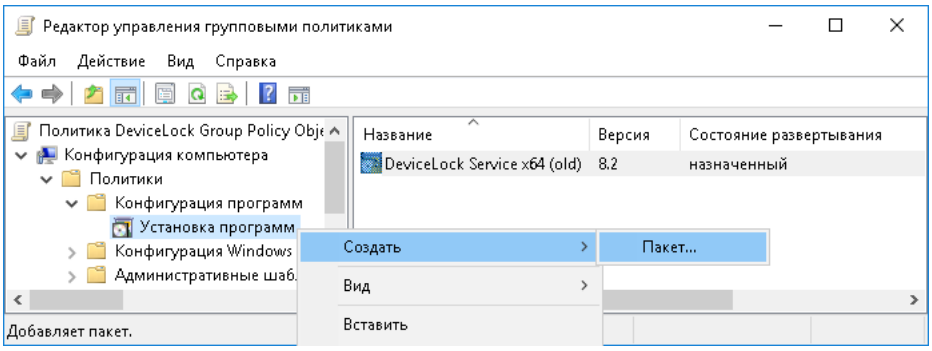


7. Закройте редактор управления групповыми политиками. Сервис DeviceLock будет установлен на компьютеры при их следующем включении.

- **Обновление пакета**

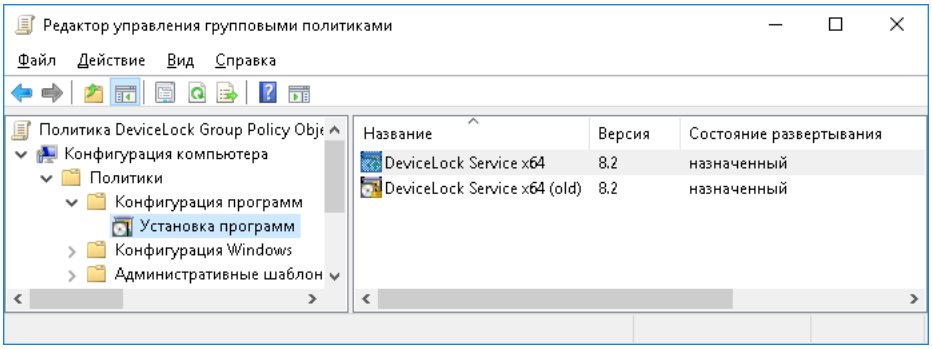
  Если предыдущая версия сервиса DeviceLock уже была установлена и требуется ее обновление путем установки новой версии:

  1. Используйте консоль “Управление групповой политикой”, чтобы открыть объект групповой политики, содержащий старый сервис DeviceLock, в редакторе управления групповыми политиками.
  2. В разделе **Конфигурация компьютера** раскройте пункт **Конфигурация программ**.
  3. Нажмите правой кнопкой мыши элемент **Установка программ**, выберите **Создать** и затем щелкните **Пакет**.

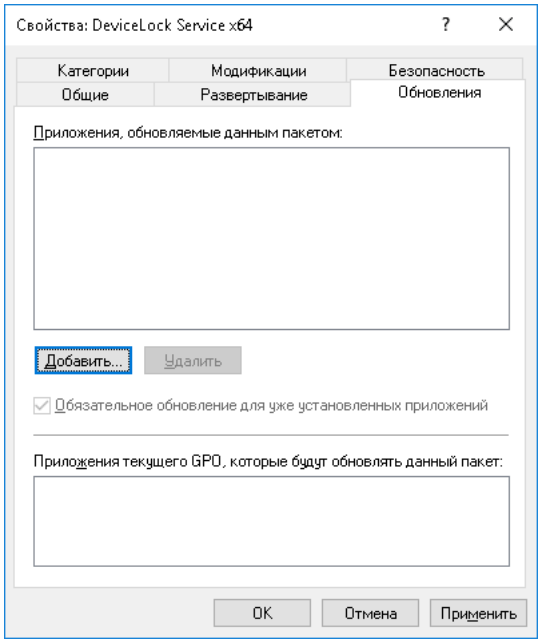


4. В диалоге **Открытие** введите полный сетевой путь (UNC) к общей сетевой папке, содержащей новый MSI-пакет.
   Пример: `\\file server\share\DeviceLock Service.msi`.
5. Нажмите **Открыть**.
6. Выберите опцию **Назначенный**, а затем нажмите **OK**.

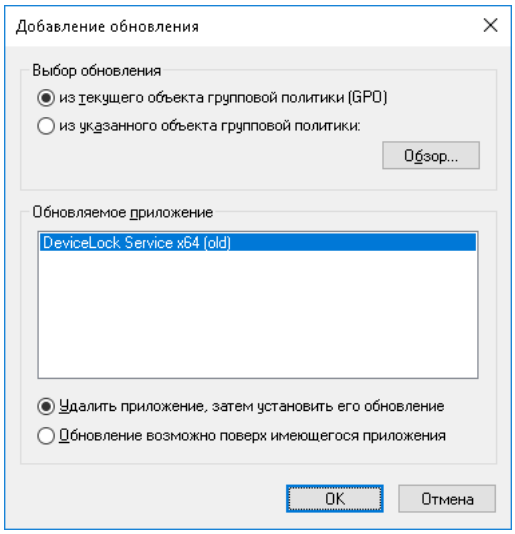
   Новый пакет будет добавлен в правую часть окна редактора управления групповыми политиками.



7. Нажмите правой кнопкой мыши новый пакет, выберите **Свойства**, а затем щелкните вкладку **Обновления**.



8. Нажмите кнопку **Добавить**, выберите старый пакет сервиса DeviceLock, который требуется обновить, выберите опцию **Удалить приложение, затем установить его обновление** и затем нажмите на **OK**.



9. Нажмите **OK**, чтобы закрыть окно **Свойства**. Затем закройте редактор управления групповыми политиками.

   Сервис DeviceLock будет обновлен на компьютерах при их следующем включении.

   Примечание: Обычно при обновлении сервиса DeviceLock новый MSI-пакет сам обнаруживает пакет для обновления в объекте групповой политики, так что действия, описанные в пунктах 7 и 8, выполняются автоматически.

- **Переустановка пакета**

  В некоторых случаях может потребоваться переустановка текущей версии сервиса DeviceLock.

  Для переустановки пакета:

  1. Используйте консоль “Управление групповой политикой”, чтобы открыть объект групповой политики, содержащий установленный сервис DeviceLock, в редакторе управления групповыми политиками.
  2. В разделе **Конфигурация компьютера** раскройте пункт **Конфигурация программ**.
  3. Выберите запись, которая соответствует установленному пакету.
  4. В правой части окна редактора управления групповыми политиками нажмите правой кнопкой мыши запись пакета, выберите **Все задачи**, затем щелкните **Развернуть приложение заново**.

     Будет показано сообщение: “Повторное развертывание этого приложение приведет к его переустановке на всех компьютерах, где оно было установлено. Вы хотите продолжить?”
  5. Нажмите **Да**.
  6. Закройте редактор управления групповыми политиками.

- **Удаление пакета**

  Чтобы удалить сервис DeviceLock:

  1. Используйте консоль “Управление групповой политикой”, чтобы открыть объект групповой политики, содержащий установленный сервис DeviceLock, в редакторе управления групповыми политиками.
  2. В разделе **Конфигурация компьютера** раскройте пункт **Конфигурация программ**.
  3. Выберите запись, которая соответствует установленному пакету.
  4. В правой части окна редактора управления групповыми политиками нажмите правой кнопкой мыши запись пакета, выберите **Все задачи**, затем щелкните **Удалить**.
  5. Выберите **Немедленное удаление этого приложения с компьютеров всех пользователей**, затем нажмите кнопку **OK**.
  6. Закройте редактор управления групповыми политиками.

Примите во внимание следующее:

- Установка и удаление происходит только при включении компьютера. Это предохраняет от нежелательных результатов, таких как удаление или обновление приложения, используемого в данный момент пользователями.
- Сервис DeviceLock будет скопирован в папку `%ProgramFiles%\DeviceLock Agent`, если он еще не установлен на этом компьютере. Если сервис DeviceLock уже установлен, но его версия ниже 7.0, сервис DeviceLock также будет скопирован в папку по умолчанию `%ProgramFiles%\DeviceLock Agent`. Если сервис DeviceLock уже установлен и его версия 7.0 или выше, то сервис DeviceLock будет скопирован в папку, где установлена эта версия, и заменит ее.

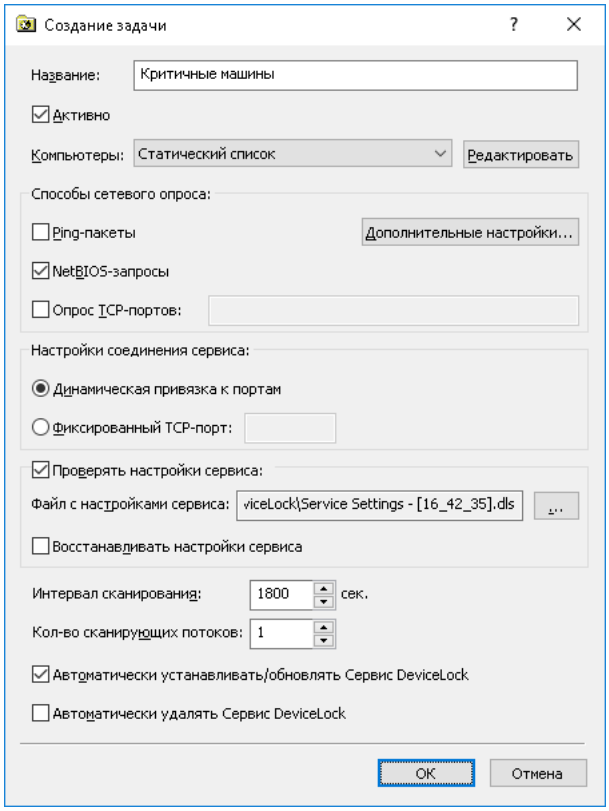
Установка с помощью DeviceLock Enterprise Server

Для установки сервиса DeviceLock можно использовать задачи мониторинга в DeviceLock Enterprise Server. При этом установка выполняется из MSI-пакета `DeviceLock Service.msi` или `DeviceLock Service x64.msi`.

Примечание: Если служба DeviceLock Enterprise Server запускается под локальной учетной записью системы (Local System), то установить, обновить или удалить сервис DeviceLock с помощью задачи мониторинга будет невозможно.

Инструкции по созданию задач мониторинга см. в разделе Создание/Редактирование задачи.

Чтобы настроить задачу для установки сервиса DeviceLock, установите флажок **Автоматически устанавливать/обновлять Сервис DeviceLock** в диалоговом окне **Создание задачи** и убедитесь, что установлен флажок **Активно**.



Чтобы настроить задачу для автоматического удаления сервиса DeviceLock, установите флажок **Автоматически удалять Сервис DeviceLock**.

При выполнении таких задач мониторинга DeviceLock Enterprise Server автоматически устанавливает и удаляет сервис DeviceLock.

Примечание: При использовании DeviceLock Enterprise Server для установки сервиса DeviceLock из пользовательского MSI-пакета, заданные настройки сервиса не применяются к клиентским компьютерам в любой из следующих ситуаций:

- Имя файла MSI-пакета отличается от `DeviceLock Service.msi` или `DeviceLock Service x64.msi`.
- Первые 3 цифры версии сервиса DeviceLock отличаются от первых 3 цифр версии DeviceLock Enterprise Server.

Инструкции по созданию пользовательского MSI-пакета см. в описании команды Создать MSI-пакет.

Развертывание сервиса DeviceLock для Mac

Для развертывания сервиса DeviceLock для Mac используется файл инсталлатора `DeviceLock Service.pkg` из образа, входящего в дистрибутив DeviceLock.

Вначале необходимо смонтировать файл образа `DeviceLock Service.dmg`.

Далее можно использовать следующие способы установки сервиса DeviceLock для Mac из этого образа:

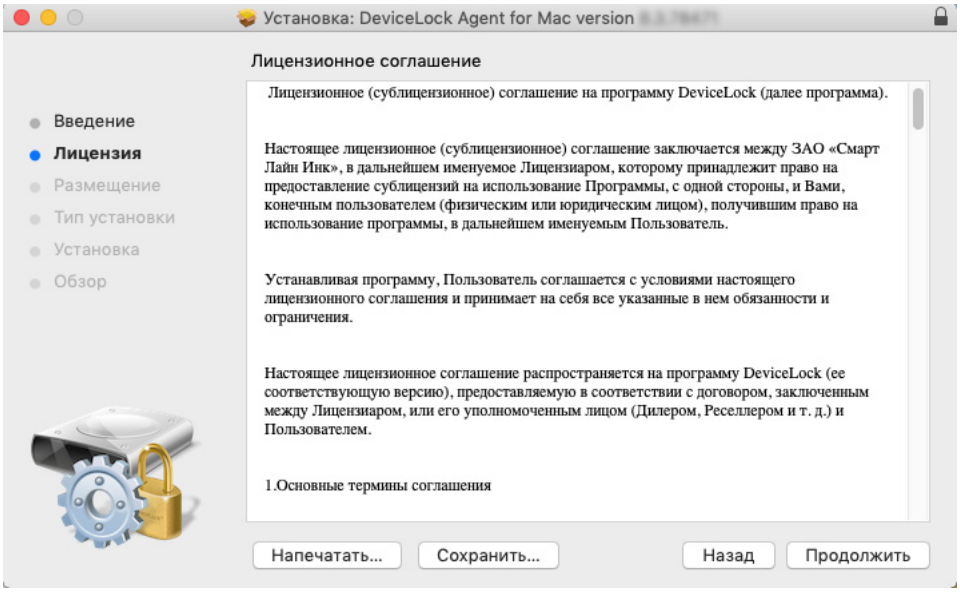
- Интерактивная установка
- Использование командной строки
- Установка без вмешательства пользователя

Интерактивная установка

Интерактивная установка начинается с запуска файла инсталлятора `DeviceLock Service.pkg`. Этот файл необходимо запускать на каждом компьютере, где должен быть установлен сервис DeviceLock для Mac. Установка новой версии сервиса поверх предыдущей требует прав администратора сервиса DeviceLock для Mac, в противном случае установка будет невозможна.

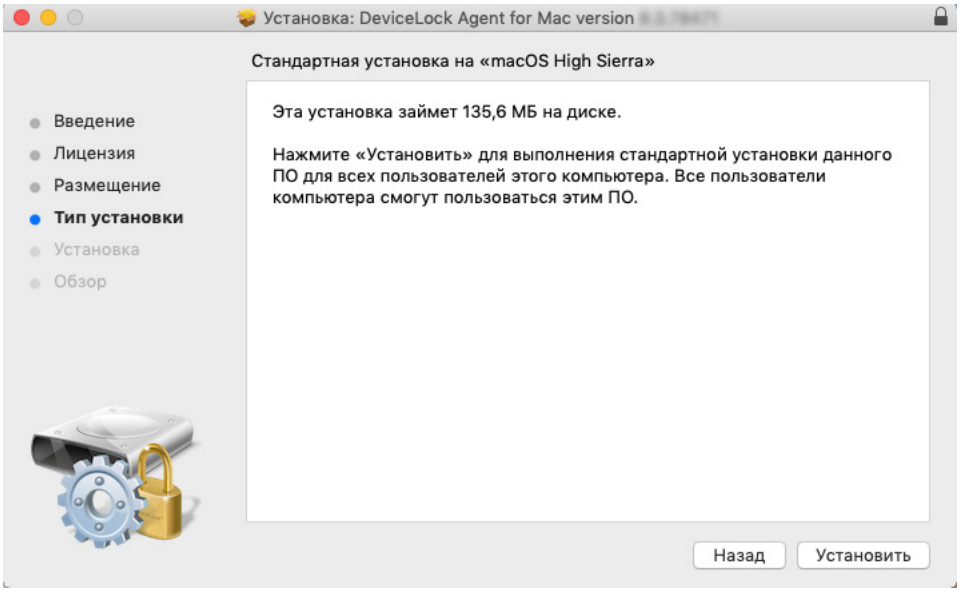
Для установки сервиса DeviceLock для Mac в интерактивном режиме запустите файл `DeviceLock Service.pkg` и следуйте инструкциям на экране.

Программа установки предложит ознакомиться с лицензионным соглашением на программное обеспечение DeviceLock. Данное лицензионное соглашение можно сохранить как текст или распечатать для дальнейшего использования. Нажмите кнопку **Продолжить** для перехода к следующему шагу установки.

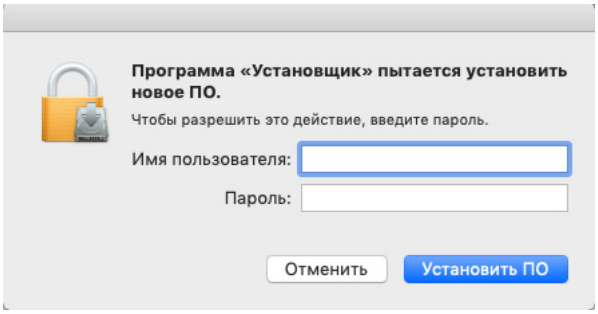


Требуется прочитать и принять лицензионное соглашение на использование программы перед тем, как продолжить установку. Нажмите кнопку **Принять** для перехода к следующему шагу установки.

Программа установки сообщит об объеме дискового пространства, который потребуется для установки сервиса DeviceLock для Mac. Теперь сервис DeviceLock для Mac готов к установке. Нажмите кнопку **Установить** для продолжения установки.



Для установки сервиса DeviceLock для Mac потребуется аутентификация с административными правами доступа. Укажите имя пользователя, обладающего административными правами доступа, и пароль, затем нажмите кнопку **Установить ПО** для продолжения установки.



В процессе установки, который может занять несколько минут, будет отображаться диалоговое окно с прогресс-баром. Прерывание установки сервиса DeviceLock для Mac не допускается. Если впоследствии потребуется удаление программы, воспользуйтесь стандартной процедурой удаления программного обеспечения.

Спустя несколько минут установка будет завершена. Нажмите кнопку **Закрыть**, чтобы закрыть программу установки.

Использование командной строки

Возможна установка с использованием утилиты командной строки, позволяющая установить сервис DeviceLock для Mac в интерактивном режиме или без вмешательства пользователя. В любом случае для установки потребуются административные права доступа к компьютеру, на котором должен быть установлен сервис DeviceLock для Mac.

Утилита командной строки находится в папке `/Library/DeviceLockAgent/Utilities/install`. Данная утилита может быть перемещена (скопирована) в любую другую папку. Файл `.pkg` должен быть размещен в той же папке. Важно копировать только один файл `.pkg`, в противном случае при запуске инсталляционного пакета без параметров может быть установлен произвольный установочный пакет.

Утилита командной строки может осуществлять установку агента как в интерактивном режиме, так и в форме "тихой" установки (без вмешательства пользователя). Используйте утилиту командной строки для установки сервиса DeviceLock для Mac, как показано далее.

Поскольку предусмотрено несколько способов установки сервиса DeviceLock для Mac, рекомендуется использование следующей команды:

```
sudo install --delayed --package <путь_к_pkg-файлу> --settings <путь_к_ini-файлу>
```

Параметр `--settings` является необязательным.

Пример:

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

Примечание: Если на компьютере, на который ведется установка сервиса DeviceLock для Mac, установлен Python 3 или более поздние версии, используйте следующую команду:

```
sudo python2.7 install --delayed --package <путь_к_pkg-файлу> --settings
<путь_к_ini-файлу>
```

- или -

```
sudo python2.6 install --delayed --package <путь_к_pkg-файлу> --settings
<путь_к_ini-файлу>
```

По умолчанию, Apple поставляет свои системы с Python 2.6 или 2.7.

Если сервис DeviceLock для Mac устанавливается впервые, указанная выше команда запустит "тихую" установку (без вмешательства пользователя). В противном случае система обновит или переустановит сервис DeviceLock для Mac после перезагрузки компьютера.

В случае переустановки или обновления сервиса DeviceLock для Mac интерактивная установка не рекомендуется, поскольку обновленная программа начнет работать только после перезагрузки.

Установка без вмешательства пользователя

Для установки сервиса DeviceLock для Mac без вмешательства пользователя потребуется использовать установочную утилиту командной строки в “тихом” режиме.

Установка без вмешательства пользователя запускается путем использования установочной утилиты с параметрами `--silent` или `--delayed` в командной строке. Параметр `--delayed` неявно задействует также параметр `--silent`. Обратите внимание, что в зависимости от наличия или отсутствия учетной записи “root” в списке администраторов DeviceLock установочная утилита может вести себя следующим образом:

- Если установочная утилита запущена без указания `.pkg` файла, будет установлен первый встретившийся файл `.pkg` в папке, где расположена установочная утилита. Если в этой папке находится несколько файлов `.pkg`, будет установлен случайно выбранный файл `.pkg`.
- Требуемый файл `.pkg` можно указать, добавив его полное имя в команду установки после параметра `--package`. Параметры могут перечисляться в любом порядке. Поддерживается относительное написание имен файлов.
- Установочная утилита будет выполнять режим “тихой” установки, если пользователь “root” не включен в список администраторов DeviceLock. В этом случае файл `.pkg` будет скопирован в папку `/Library/DeviceLockPackages`. Сервис DeviceLock будет установлен или обновлен при очередной перезагрузке компьютера.

Можно обеспечить автоматическую настройку сервиса DeviceLock для Mac сразу после его установки с помощью специального конфигурационного файла `devicelock.ini`, в котором можно предварительно задать параметры установки сервиса. Чтобы задать настройки сервиса DeviceLock для Mac в процессе установки, укажите в файле `devicelock.ini` путь к файлу с настройками (.dls-файл). Допускается использование локального или сетевого пути к файлу.

Пример:

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

Примечание: Формат файла `devicelock.ini` для Mac такой же, как для Windows (см. раздел Установка без вмешательства пользователя для Windows), с той разницей, что действует только параметр `SettingsFile`. Этот параметр указывает имя и путь файла настроек `.dls`, который будет использоваться для настройки сервиса DeviceLock сразу после установки.

Установка консолей управления

Консоли служат для дистанционного управления сервисом DeviceLock, сервером DeviceLock Enterprise Server и сервером DeviceLock Content Security Server.

Консоли управления устанавливают на компьютере, с которого будут управлять сервисом DeviceLock и серверами DeviceLock, установленными на других компьютерах. При этом не требуется устанавливать консоли управления на какой-либо сервер (например, контроллер домена). Даже если планируется использовать DeviceLock Group Policy Manager для управления настройками DeviceLock через групповые политики Active Directory, администратор может делать это со своего рабочего компьютера (при наличии необходимых прав доступа в домене Active Directory).

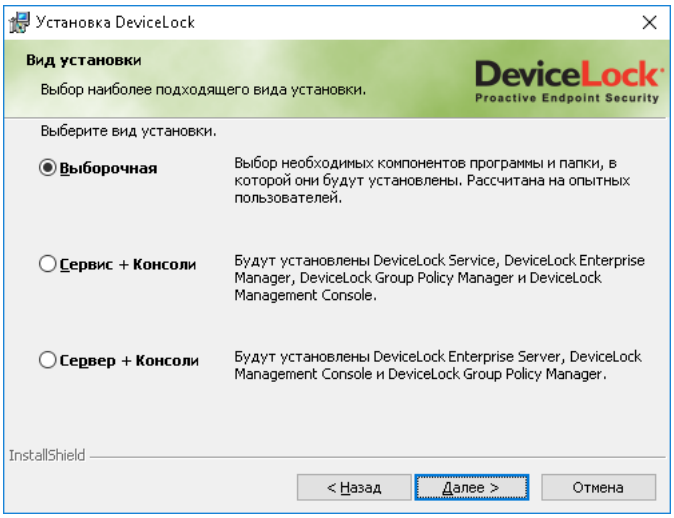
Примечание: DeviceLock Group Policy Manager интегрируется в редактор управления групповыми политиками Windows и недоступен как отдельное приложение. Для его использования нужно открыть объект групповой политики в этом редакторе.

Запустите программу установки `setup.exe` и следуйте инструкциям на страницах мастера установки.

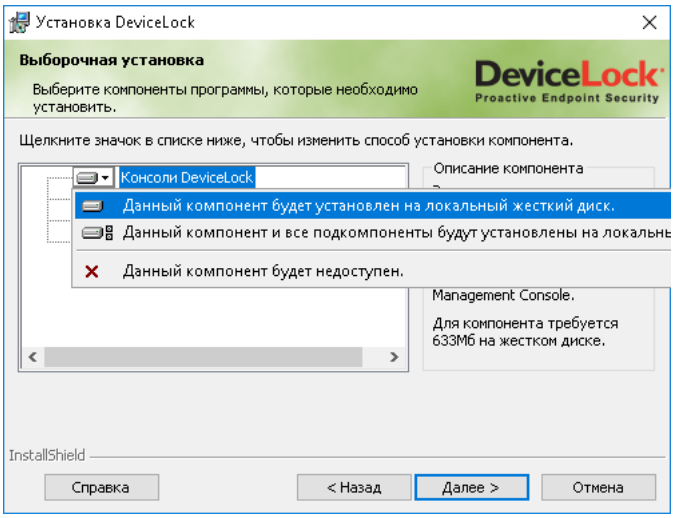
На странице **Лицензионное соглашение** ознакомьтесь с лицензионным соглашением и выберите опцию **Я принимаю условия лицензионного соглашения**, чтобы принять условия лицензионного соглашения и продолжить установку.

На странице **Сведения о пользователе** введите свое имя и название организации.

На странице **Вид установки** выберите требуемый тип установки.



Можно установить сервис DeviceLock и консоли управления DeviceLock, выбрав опцию **Сервис + Консоли**; установить DeviceLock Enterprise Server и консоли управления, выбрав опцию **Сервер + Консоли** или установить только консоли управления, выбрав опцию **Выборочная** и затем отметив компонент **Консоли DeviceLock**.

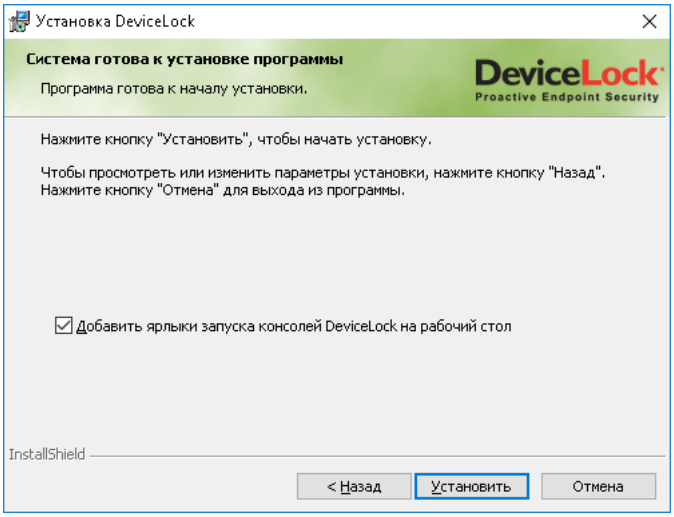


Примечание: На странице **Выборочная установка** можно также выбрать для установки компонент RSoP. Этот компонент обеспечивает поддержку режима планирования результирующей политики (RSoP) DeviceLock на контроллерах домена. Компонент RSoP необходим только тогда, когда на компьютере установлены консоли управления DeviceLock, но не установлен сервис DeviceLock. Описание режима планирования RSoP можно найти в документации Microsoft по адресу technet.microsoft.com/library/cc758010.aspx.

На странице **Выборочная установка** можно изменить папку установки. Для этого нажмите кнопку **Изменить** и выберите папку в появившемся диалоговом окне. Папка установки по умолчанию: `%ProgramFiles%\DeviceLock`.

DeviceLock содержит три консоли управления: DeviceLock Management Console, DeviceLock Enterprise Manager, и DeviceLock Group Policy Manager (интегрируется в редактор управления групповыми политиками Windows). Вместе с консолями управления устанавливается редактор DeviceLock Service Settings Editor, который служит для создания и редактирования файлов с настройками, разрешениями, а также правилами аудита, теневого копирования и тревожных оповещений для сервиса DeviceLock (файлы настроек сервиса DeviceLock).

На странице **Система готова к установке программы** нажмите кнопку **Установить**, чтобы начать установку. Установите флажок **Добавить ярлыки запуска консолей DeviceLock на рабочий стол**, чтобы добавить ярлыки запуска консолей DeviceLock Management Console (оснастка MMC), DeviceLock Enterprise Manager и DeviceLock Service Settings Editor на рабочий стол.



Программа установки может предложить создание сертификата DeviceLock. Появится следующее сообщение: “Вы хотите создать новый сертификат DeviceLock (открытый и секретный ключи)? Нажмите “Нет”, если у Вас уже есть сертификат DeviceLock и не нужно создавать новую пару ключей.”

Сертификаты можно создавать с помощью мастера создания сертификата (см. Сертификаты DeviceLock далее в этом документе). Этот мастер устанавливается вместе с консолями управления DeviceLock. Поэтому, если в данный момент нет уверенности, нужен ли новый сертификат, нажмите кнопку **Нет** и продолжайте установку.

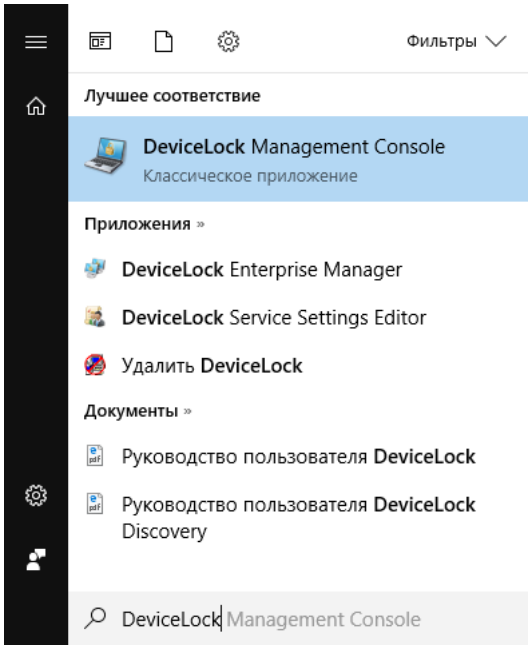
Программа установки может запросить файлы лицензий DeviceLock. При отсутствии этих файлов нажмите кнопку **Отмена**, чтобы установить DeviceLock в ознакомительном 30-дневном режиме. Подробнее см. в разделе Активация клиентских лицензий.

Если была выбрана установка консолей вместе с сервисом DeviceLock, программа установки предложит задать разрешения для локальных устройств и протоколов (см. описание настроек в разделе Интерактивная установка для сервиса DeviceLock ранее в этом документе). Чтобы установить сервис DeviceLock без применения этих настроек, нажмите кнопку **Пропустить**. Просмотреть или изменить настройки можно будет с помощью консоли управления DeviceLock.

Если была выбрана установка консолей вместе с сервером DeviceLock Enterprise Server, программа установки запустит мастер настройки сервера. Описание этого мастера приведено в разделе Инструкции по установке для DeviceLock Enterprise Server далее в этом документе.

На странице **Мастер установки завершен** нажмите кнопку **Готово**, чтобы завершить процесс установки. С завершающей страницы мастера можно перейти на веб-сайт DeviceLock. Этот вариант выбран по умолчанию.

Команды запуска консолей управления доступны на стартовой странице Windows:



Примечание: Удалить DeviceLock можно следующим образом:

- Используйте средство **Программы и компоненты** панели управления Windows (**Установка и удаление программ** на ранних версиях Windows).

  - или -
- Выберите пункт **Удалить DeviceLock** в меню **Пуск** Windows.

Установка DeviceLock Enterprise Server

Сервер DeviceLock Enterprise Server - это дополнительный компонент, предназначенный для централизованного сбора и хранения данных теневого копирования и журналов DeviceLock. С его помощью можно также централизованно отслеживать состояние сервиса DeviceLock на удаленных компьютерах путем их периодического опроса.

DeviceLock Enterprise Server можно установить на нескольких компьютерах в локальной сети с целью равномерного распределения нагрузки на каждый из них и на всю сеть в целом.

Для хранения данных DeviceLock Enterprise Server используется сервер базы данных. Поэтому такой сервер должен быть запущен в локальной сети перед установкой DeviceLock Enterprise Server. В качестве сервера базы данных может служить, например, Microsoft SQL Server Express, который можно свободно скачать по адресу go.microsoft.com/fwlink/?LinkID=799012.

Сервер базы данных и сервер DeviceLock Enterprise Server могут быть установлены на разных компьютерах. Поскольку такое решение повышает производительность и надежность всей системы, рекомендуется устанавливать DeviceLock Enterprise Server на отдельный компьютер.

Предусмотрены три варианта сопряжения сервера DeviceLock Enterprise Server и сервера базы банных. Перед установкой DeviceLock Enterprise Server выберите подходящий для вас вариант:

1. ОДИН К ОДНОМУ - Устанавливается один сервер DeviceLock Enterprise Server с подключением к одному серверу базы данных. Этот вариант подходит для небольших сетей (до нескольких сотен компьютеров).
2. МНОГИЕ КО МНОГИМ - Устанавливаются несколько серверов DeviceLock Enterprise Server с подключением каждого к отдельному серверу базы данных. Этот вариант подходит для средних и крупных сетей, разделенных на несколько сегментов и имеющих медленные соединения между этими сегментами.
3. МНОГИЕ К ОДНОМУ - Устанавливаются несколько серверов DeviceLock Enterprise Server с подключением всех к единому серверу базы данных. Этот вариант подходит для средних и крупных сетей, где сервер базы данных для различных приложений развернут на отдельном сервере с большим объемом оперативной памяти и дискового пространства.

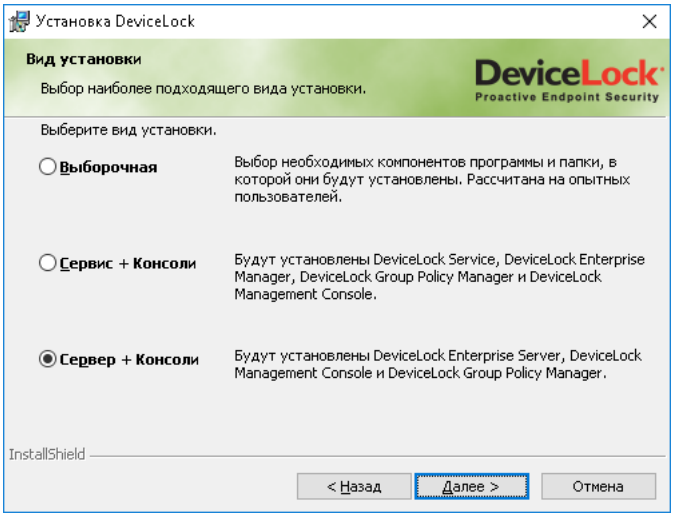
Инструкции по установке

На каждом компьютере, где предполагается установить DeviceLock Enterprise Server, запустите программу установки `setup.exe` и следуйте инструкциям в мастере установки.

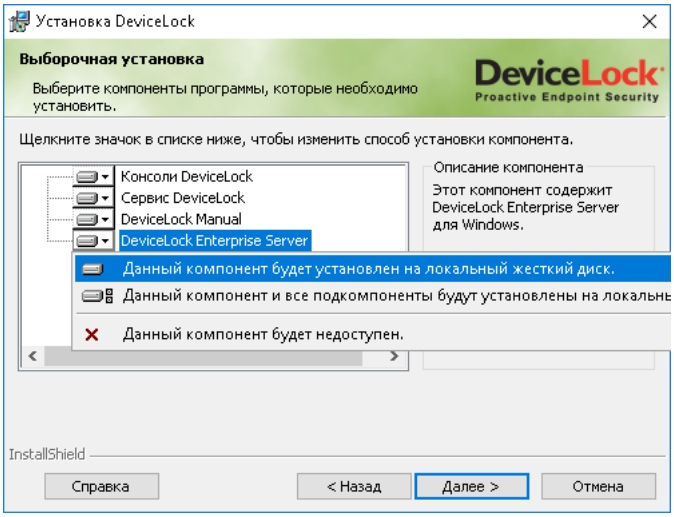
На странице **Лицензионное соглашение** ознакомьтесь с лицензионным соглашением и выберите опцию **Я принимаю условия лицензионного соглашения**, чтобы принять условия лицензионного соглашения и продолжить установку.

На странице **Сведения о пользователе** введите свое имя и название организации.

На странице **Вид установки** выберите требуемый тип установки.



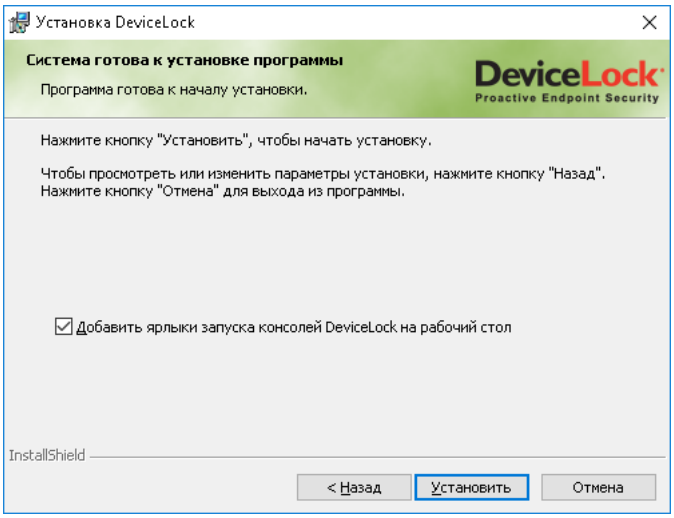
Можно установить DeviceLock Enterprise Server и консоли управления DeviceLock, выбрав опцию **Сервер + Консоли** или установить только DeviceLock Enterprise Server, выбрав опцию **Выборочная** и затем отметив компонент **DeviceLock Enterprise Server**.



Примечание: На странице **Выборочная установка** можно также выбрать компонент RSoP. Этот компонент обеспечивает поддержку режима планирования результирующей политики (RSoP) DeviceLock на контроллерах домена. Компонент RSoP необходим только если на компьютере установлены консоли управления DeviceLock, но не установлен сервис DeviceLock. Описание режима планирования RSoP можно найти в документации Microsoft по адресу technet.microsoft.com/library/cc758010.aspx.

На странице **Выборочная установка** можно изменить папку установки. Для этого нажмите кнопку **Изменить** и выберите папку в появившемся диалоговом окне. Папка установки по умолчанию: `%ProgramFiles%\DeviceLock`.

На странице **Система готова к установке программы** нажмите кнопку **Установить**, чтобы начать установку. Установите флажок **Добавить ярлыки запуска консолей DeviceLock на рабочий стол**, чтобы добавить ярлыки запуска консолей DeviceLock Management Console, DeviceLock Enterprise Manager и DeviceLock Service Settings Editor на рабочий стол.



Если выбрана установка консолей управления DeviceLock, программа установки может предложить создание сертификата DeviceLock. Появится следующее сообщение: “Вы хотите создать новый сертификат DeviceLock (открытый и секретный ключи)? Нажмите “Нет”, если у Вас уже есть сертификат DeviceLock и не нужно создавать новую пару ключей.”

Сертификаты можно создавать с помощью мастера создания сертификата (см. Сертификаты DeviceLock далее в этом документе). Этот мастер устанавливается вместе с консолями управления DeviceLock. Поэтому, если в данный момент нет уверенности, нужен ли новый сертификат, нажмите кнопку **Нет** и продолжайте установку.

При отсутствии SQL Server на локальном компьютере программа установки может предложить его установку. Появится следующее сообщение: “SQL Server не запущен на локальном компьютере. Вы хотите его установить?”

Если устанавливать SQL Server на локальный компьютер не нужно, или он уже установлен, но не запущен, нажмите кнопку **Нет** и продолжайте установку.

В процессе установки потребуется настроить DeviceLock Enterprise Server, задав его основные параметры в мастере настройки.

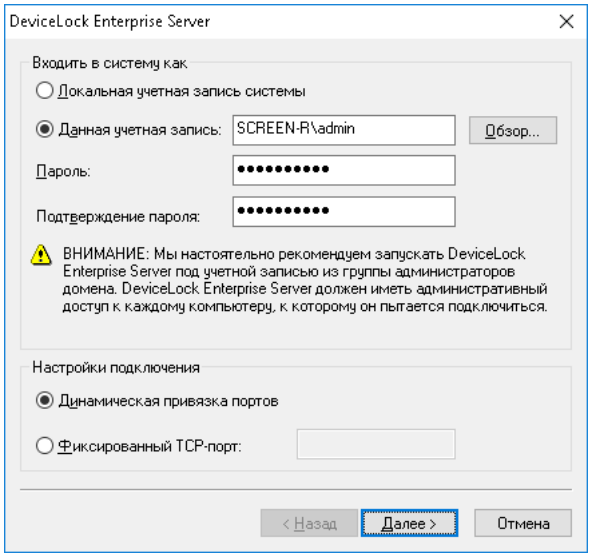
Если вы устанавливаете обновление DeviceLock Enterprise Server или переустанавливаете его и при этом не хотите ничего менять в текущих настройках, нажмите кнопку **Далее**, и затем нажмите кнопку **Отмена**, чтобы закрыть мастер и сохранить все текущие настройки.

Если требуется изменить какие-либо параметры, сохраняя все остальные настройки, измените только необходимые параметры, пройдите через все страницы мастера настройки и нажмите кнопку **Готово** на последней странице.

Примечание: Если вы устанавливаете DeviceLock Enterprise Server в первый раз на данный компьютер и при этом закрываете мастер настройки, не задав параметры запуска службы DeviceLock Enterprise Server, программа установки не сможет настроить эту службу, и будет снова предложено использовать мастер настройки. Появится следующее сообщение: “Мастер настройки был прерван до того, как DeviceLock Enterprise Server был полностью настроен. Вы хотите запустить мастер настройки снова (нажмите “Нет” для продолжения процесса установки без настройки DeviceLock Enterprise Server)?” Если нажать **Нет** для продолжения без установки службы DeviceLock Enterprise Server, то впоследствии потребуется снова запустить программу установки, чтобы настроить эту службу.

Учетная запись службы и параметры подключения

На первой странице мастера настройки задается учетная запись запуска службы DeviceLock Enterprise Server и выбирается TCP-порт для подключения к этому серверу.



Входить в систему как

Необходимо задать учетную запись для запуска службы DeviceLock Enterprise Server. Это может быть локальная учетная запись системы или другая учетная запись.

Для запуска службы под учетной записью системы, выберите опцию **Локальная учетная запись системы**. Следует помнить, что программы, работающие под этой учетной записью, не могут получить доступ к сетевым ресурсам и авторизуются на удаленных компьютерах как анонимный непривилегированный пользователь. Таким образом, DeviceLock Enterprise Server, запущенный под локальной учетной записью системы, не сможет хранить файлы теневого копирования на удаленных компьютерах (например, на файловых серверах) и должен будет авторизоваться с помощью сертификата DeviceLock для доступа к сервису DeviceLock на удаленных компьютерах.

Дополнительную информацию о методах авторизации можно найти в описании параметра Имя сертификата.

Примечание: Если служба DeviceLock Enterprise Server запускается под учетной записью системы, то задачи мониторинга, исполняемые на таком сервере, не могут устанавливать, обновлять и удалять сервис DeviceLock на удаленных компьютерах.

Для запуска службы под другой учетной записью выберите опцию **Данная учетная запись** и введите имя пользователя и его пароль. Рекомендуется использовать учетную запись пользователя с правами администратора на всех компьютерах, где работает сервис DeviceLock. В противном случае для авторизации потребуется использовать сертификат DeviceLock.

При установке DeviceLock Enterprise Server в домене Active Directory для запуска службы рекомендуется использовать учетную запись, включенную в группу администраторов домена (Domain Admins). В результате служба получит права администратора на всех компьютерах данного домена, поскольку группа администраторов домена по умолчанию входит в локальную группу администраторов на каждом компьютере, подключенном к домену.

Необходимо также учитывать, что при включенной защите сервиса DeviceLock от локального администратора (снят флажок **Включить безопасность по умолчанию** для администраторов DeviceLock) учетная запись, указанная в параметре **Данная учетная запись**, должна быть в списке администраторов DeviceLock с правом **Полный доступ**. В противном случае потребуется использовать авторизацию на основе сертификата DeviceLock.

Настройки подключения

DeviceLock Enterprise Server можно настроить на использование определенного TCP-порта для связи с консолью управления: выберите опцию **Фиксированный TCP-порт** и введите номер порта. Для автоматического выбора порта выберите опцию **Динамическая привязка портов**. По умолчанию DeviceLock Enterprise Server использует порт 9133.

Нажмите на кнопку **Далее**, чтобы запустить службу DeviceLock Enterprise Server и перейти на вторую страницу мастера настройки.

Запуск службы DeviceLock Enterprise Server

Если пользователь, запустивший мастер настройки, не является администратором DeviceLock Enterprise Server (в ситуации, когда устанавливается обновление поверх уже настроенного сервера), мастер настройки не сможет установить службу сервера и внести изменения в его параметры. Появится следующее сообщение: "Доступ запрещен." Та же ошибка возникает, если этот пользователь не обладает правами администратора на компьютере, где выполняется установка DeviceLock Enterprise Server.

Если для параметра **Данная учетная запись** указано несуществующее имя пользователя или неправильно введен пароль, то операционная система не сможет запустить службу DeviceLock Enterprise Server. Появится следующее сообщение: "Имя учетной записи задано неверно или не существует, или же неверен указанный пароль."

Если учетная запись, указанная в параметре **Данная учетная запись**, не является членом группы администраторов домена (Domain Admins), появится следующее сообщение: "Учетная запись <имя> не принадлежит к группе администраторов домена. Вы хотите продолжить?"

Можно продолжить, нажав на кнопку **Да**. При этом указанной учетной записи должны быть предоставлены права администратора на удаленных компьютерах, на которых работает сервис DeviceLock. В противном случае на таких компьютерах потребуется установить открытый ключ сертификата DeviceLock.

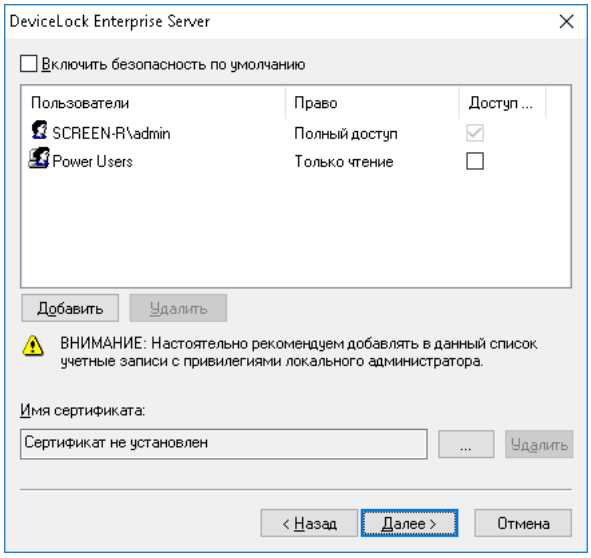
Если учетная запись, указанная для параметра **Данная учетная запись**, не обладает системной привилегией "Входить в систему как служба", мастер настройки автоматически присвоит ей эту привилегию. Данная привилегия необходима для запуска службы под учетной записью пользователя. Появится следующее сообщение: "Для учетной записи <имя> добавлено право входить в систему как служба."

Если параметры запуска заданы верно, выполняется запуск службы. Появляется следующее сообщение: "Пожалуйста, подождите, пока программа взаимодействует со службой. Запуск службы DLServer на компьютере: Локальный компьютер…"

Запуск службы DeviceLock Enterprise Server занимает некоторое время (около минуты), после чего отображается вторая страница мастера настройки.

Администраторы сервера и сертификат

На второй странице мастера можно задать список администраторов сервера DeviceLock Enterprise Server, а также установить секретный ключ сертификата DeviceLock.



Включить безопасность по умолчанию

При контроле доступа к DeviceLock Enterprise Server по умолчанию любые пользователи, обладающие правами локального администратора, могут подключаться к DeviceLock Enterprise Server с помощью консоли управления, изменять его настройки и просматривать отчеты.

Чтобы включить контроль доступа по умолчанию, установите флажок **Включить безопасность по умолчанию**.

Если требуется более гибкий контроль доступа к DeviceLock Enterprise Server, отключите контроль по умолчанию, сняв флажок **Включить безопасность по умолчанию**.

Если флажок **Включить безопасность по умолчанию** снят, нужно задать список учетных записей (пользователей и/или групп), которые смогут подключаться к DeviceLock Enterprise Server. Чтобы добавить учетную запись в этот список, нажмите кнопку **Добавить**. Можно добавить несколько учетных записей одновременно.

Для удаления учетных записей из списка используйте кнопку **Удалить**. Используя клавишу Ctrl или Shift, можно выбрать и удалить несколько записей одновременно.

Чтобы установить, какие действия разрешены пользователю или группе, выберите требуемый уровень доступа к серверу:

- **Полный доступ** - Позволяет устанавливать и удалять сервер DeviceLock Enterprise Server, подключаться к нему с помощью консоли DeviceLock Management Console и выполнять любые действия на сервере, в том числе просматривать и изменять настройки сервера, создавать, редактировать и запускать задачи мониторинга и задачи создания отчетов, просматривать отчеты, а также выполнять настройку политик.
- **Изменение** - То же, что и полный доступ к серверу, за исключением права вносить изменения в список администраторов сервера, а также права изменять уровень доступа к серверу для пользователей и групп, уже имеющихся в этом списке.
- **Только чтение** - Позволяет подключаться к серверу DeviceLock Enterprise Server с помощью консоли DeviceLock Management Console, просматривать настройки сервера, а также запускать задачи создания отчетов и просматривать отчеты. Не позволяет вносить какие-либо изменения на сервере, создавать, редактировать и запускать задачи мониторинга, создавать и редактировать задачи создания отчетов, выполнять настройку политик.

Для пользователей и групп с уровнем доступа **Изменение** или **Только чтение** можно выбрать опцию **Доступ к теневым копиям**, чтобы обеспечить доступ к теневым копиям и записям активности пользователей. Пользователи и группы, для которых выбрана эта опция, могут просматривать, открывать и сохранять теневые копии и записи активности пользователей из журналов сервера DeviceLock Enterprise Server, используя средства просмотра журнала теневого копирования (см. Просмотрщик журнала теневого копирования (для сервера)) и журнала активности пользователей (см. Просмотр активности пользователей).

Администраторам сервера DeviceLock Enterprise Server, не имеющим доступа к теневым копиям, недоступно содержимое теневых копий и записей активности пользователей. Они не могут открывать, просматривать и сохранять теневые копии и записи активности пользователей.

Внимание: Настоятельно рекомендуется предоставить администраторам сервера DeviceLock Enterprise Server права локального администратора, поскольку при установке, обновлении или удалении сервера DeviceLock Enterprise Server может потребоваться доступ к диспетчеру управления службами Windows (Service Control Manager) и общим сетевым ресурсам.

Имя сертификата

Чтобы использовать авторизацию на основе сертификата DeviceLock, на DeviceLock Enterprise Server нужно установить секретный ключ этого сертификата.

Предусмотрены два метода авторизации сервера DeviceLock Enterprise Server на удаленных компьютерах с работающим сервисом DeviceLock:

- **Авторизация по пользователю** - Служба DeviceLock Enterprise Server запущена под учетной записью, обладающей правами администратора DeviceLock на удаленном компьютере. Инструкции по выбору учетной записи для запуска службы DeviceLock Enterprise Server см. в описании параметра Входить в систему как.
- **Авторизация по сертификату** - Если учетная запись, используемая для запуска службы DeviceLock Enterprise Server не обладает правами администратора DeviceLock на удаленном компьютере, необходимо использовать авторизацию на основе сертификата DeviceLock.

  Для авторизации по сертификату нужно установить открытый ключ сертификата на сервисе DeviceLock, а соответствующий ему секретный ключ - на сервере DeviceLock Enterprise Server.

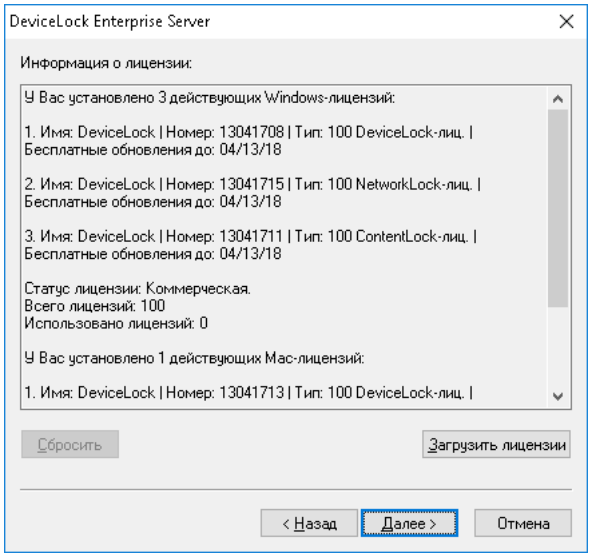
Чтобы установить сертификат, нажмите на кнопку ... и выберите файл с секретным ключом. Чтобы удалить сертификат, нажмите на кнопку **Удалить**.

Подробнее о сертификатах см. в разделе Сертификаты DeviceLock данного руководства.

Нажмите на кнопку **Далее**, чтобы применить настройки и перейти к третьей странице мастера настройки.

Информация о лицензии

Данная страница служит для установки лицензий на DeviceLock.



Лицензию, приобретенную для DeviceLock, нужно установить на DeviceLock Enterprise Server.

DeviceLock Enterprise Server работает только с тем количеством компьютеров с установленным сервисом DeviceLock, которое указано в лицензии. Например, если в лицензии указано 100 компьютеров, а в локальной сети присутствует 101 компьютер с установленным сервисом DeviceLock, то DeviceLock Enterprise Server будет работать только со 100 компьютерами, игнорируя 101-й компьютер.

Чтобы установить лицензию, нажмите на кнопку **Загрузить лицензии** и выберите файл с лицензией. Можно загрузить несколько файлов подряд - один за другим.

После загрузки файлов можно просмотреть сводную информацию о лицензии: в строке **Всего лицензий** отображается общее количество приобретенных лицензий, а строка **Использовано лицензий** содержит количество лицензий, используемых для сбора данных аудита, теневого копирования и мониторинга в DeviceLock Enterprise Server.

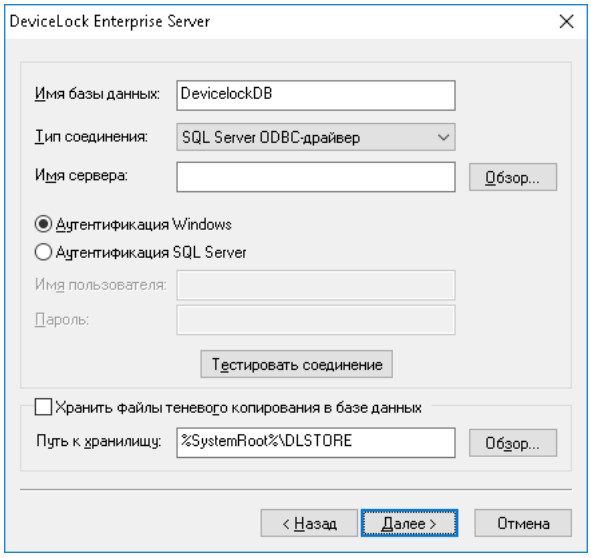
Если не установлено ни одной действительной лицензии, то DeviceLock Enterprise Server работает в ознакомительном режиме и может обслуживать только два компьютера с установленным сервисом DeviceLock.

Примечание: Если компьютер с установленным сервисом DeviceLock отключится от локальной сети, DeviceLock Enterprise Server сможет обработать его замену только после перезагрузки или по истечении 6 часов.

Нажмите на кнопку **Далее**, чтобы установить лицензии и перейти к четвертой странице мастера настройки.

Настройка базы данных

Следующая страница используется для настройки базы данных сервера DeviceLock Enterprise Server.



Имя базы данных

В поле **Имя базы данных** укажите имя базы данных для сервера DeviceLock Enterprise Server. Мастер настройки по умолчанию предлагает имя **DeviceLockDB**.

Примечание: Не следует вручную создавать базу данных с указанным именем; мастер настройки сам создает базу данных или использует уже существующую.

Тип соединения

В списке **Тип соединения** можно выбрать подходящий вариант соединения с базой данных. Предусмотрены следующие варианты:

- **SQL Server ODBC-драйвер** - Подключение к серверу Microsoft SQL Server с помощью драйвера ODBC.

  В параметре **Имя сервера** указывается имя, обычно содержащее две части: короткое имя компьютера, за которым следует имя экземпляра SQL Server, отделенное обратной косой чертой (например, `computer\instance`). Для экземпляра SQL Server по умолчанию в качестве имени сервера используется короткое имя компьютера (имя экземпляра отсутствует).

  Чтобы получить имена серверов SQL Server, доступных в локальной сети, нажмите кнопку **Обзор**. Для получения имени сервера требуется удаленный доступ к реестру компьютера, на котором работает SQL Server.

  Если параметр **Имя сервера** не задан, то считается, что выбран экземпляр SQL Server по умолчанию, работающий на компьютере, на котором установлен DeviceLock Enterprise Server.

Для доступа к SQL Server необходимо также настроить параметры аутентификации.

Выберите опцию **Аутентификация Windows** для доступа к SQL Server от имени учетной записи, под которой запущена служба DeviceLock Enterprise Server.

Если служба запущена под локальной учетной записью системы, а SQL Server находится на другом компьютере, DeviceLock Enterprise Server не сможет получить доступ к SQL Server, т.к. локальная учетная запись системы не имеет права на доступ к сетевым ресурсам. Подробнее о выборе учетной записи для службы DeviceLock Enterprise Server см. в описании параметра Входить в систему как.

Выберите опцию **Аутентификация SQL Server** для доступа к SQL Server от имени заданного пользователя SQL Server. Прежде чем выбрать эту опцию, убедитесь, что SQL Server был настроен для работы в смешанном режиме аутентификации. Укажите имя пользователя SQL Server в параметре **Имя пользователя** и соответствующий ему пароль в параметре **Пароль**.

Примечание: Аутентификация Windows обеспечивает более высокий уровень безопасности по сравнению с аутентификацией SQL Server, так что по возможности следует использовать аутентификацию Windows.

- **PostgreSQL ODBC-драйвер** - Подключение к серверу PostgreSQL с помощью драйвера PostgreSQL ODBC версии 9.6.500 или выше. Драйвер можно скачать на сайте PostgreSQL по адресу postgresql.org/ftp/odbc/versions/msi.

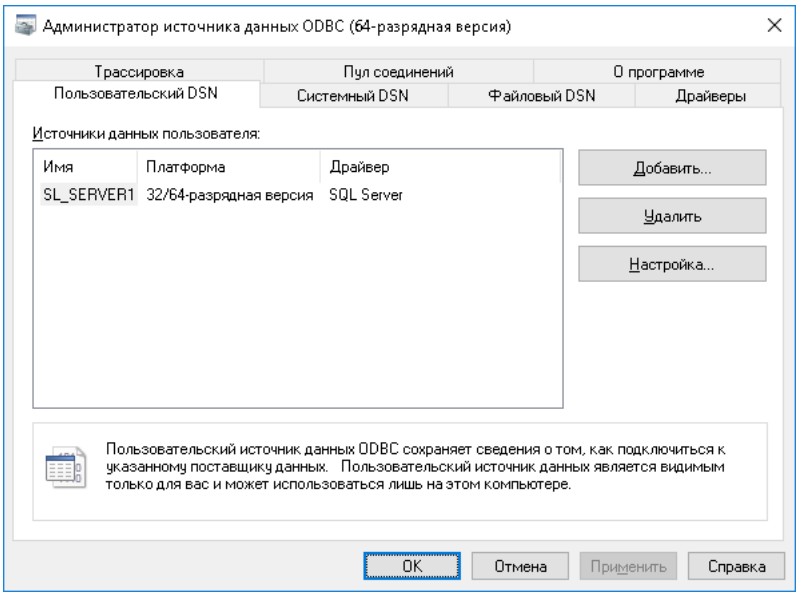
  Параметр **Имя сервера** указывает имя компьютера, на котором работает PostgreSQL. Если этот параметр не задан, то предполагается, что PostgreSQL работает на том же компьютере, что и DeviceLock Enterprise Server.

  Параметр **Имя пользователя** указывает имя пользователя PostgreSQL, а поле **Пароль** служит для ввода пароля этого пользователя. Мастер настройки обращается к серверу PostgreSQL от имени указанного пользователя для создания/обновления базы данных, поэтому необходимо выбирать пользователя с достаточными правами доступа. От имени этого пользователя выполняются также операции чтения/записи в базе данных во время работы DeviceLock Enterprise Server.

  Примечание: Если ODBC-драйвер для PostgreSQL Server не установлен или устарел, можно продолжить установку DeviceLock Enterprise Server без настройки базы данных, после чего установить необходимый ODBC-драйвер и настроить базу данных в консоли DeviceLock Management Console (см. Администрирование сервера DeviceLock Enterprise Server).

- **Системный источник данных** - Подключение к серверу базы данных с помощью ранее созданного системного источника данных. Выберите источник данных из списка **Имя источника данных**.

  Чтобы создать источник данных, используйте компонент **Администратор источника данных ODBC** в разделе **Панель управления** > **Администрирование**.



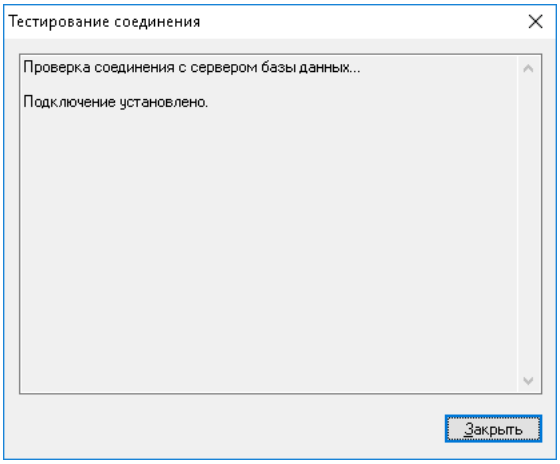
  Если источник данных требует имя пользователя и пароль (например, в случае режима аутентификации SQL Server или при подключении к PostgreSQL), необходимо указать имя пользователя и его пароль в поле **Имя пользователя** и **Пароль**, соответственно. В противном случае оставьте пустыми оба эти поля.

  Чтобы обновить список **Имя источника данных**, нажмите кнопку **Обновить**.

Проверка соединения

Задав параметры соединения, можно выполнить проверку, чтобы убедиться в их корректности. Для этого нажмите кнопку **Тестировать соединение**.

Проверяется только соединение с сервером базы данных. В случае успешного подключения к серверу диалоговое окно **Тестирование соединения** не покажет никаких ошибок, даже при наличии каких-либо проблем с базой данных или доступом к ней.



Если не удается установить соединение с использованием заданных параметров, в диалоговом окне могут появиться следующие сообщения об ошибках:

- **SQL Server does not exist or access denied** - Указано неправильное имя в параметре **Имя сервера**, либо компьютер, на котором работает SQL Server, недоступен. Возможно, указано имя компьютера, но не указано имя экземпляра SQL Server (имя нужно указывать в формате computer\instance).
- **Login failed for user 'COMPUTER_NAME$'** - Выбран режим аутентификации Windows, но учетная запись, под которой запущена служба DeviceLock Enterprise Server, не может получить доступ к SQL Server. Возможно служба запущена под локальной учетной записью системы или под учетной записью, не обладающей правами администратора на компьютере SQL Server.
- **Login failed for user 'user_name'** - Выбран режим аутентификации SQL Server, но неверно задано имя пользователя SQL Server (логин) или его пароль. В параметре **Имя пользователя** должно быть указано имя пользователя SQL Server, а не пользователя Windows. Для администрирования пользователей SQL Server используются средства SQL Server (такие как Microsoft SQL Server Management Studio).
- **Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection** - Выбран режим аутентификации SQL Server, но SQL Server не поддерживает данный режим. Необходимо либо использовать режим аутентификации Windows, либо настроить SQL Server для работы в смешанном режиме аутентификации.
- **Login failed for user ''. The user is not associated with a trusted SQL Server connection** - Источник данных, указанный в параметре **Имя источника данных** настроен для работы в режиме аутентификации SQL Server, но параметр **Имя пользователя** не задан.
- **Data source name not found and no default driver specified** - Задано неправильное значение параметра **Имя источника данных** (например, пустая строка).

Хранить файлы теневого копирования в базе данных

Хранить данные теневого копирования можно в файлах на диске либо в базе данных сервера. Для хранения их в базе данных сервера установите флажок **Хранить файлы теневого копирования в базе данных**.

Если данные теневого копирования хранятся в базе данных на сервере Microsoft SQL Server, необходимо существенно увеличить максимальный размер файла с журналом транзакций для этой базы данных. Иначе возможна некорректная обработка больших объемов данных в одной транзакции. Для наилучших результатов используйте 64-разрядный SQL Server, увеличив ему размер оперативной памяти. На 32-разрядном компьютере включите режим AWE (Address Windowing Extensions). Инструкции см. в статье technet.microsoft.com/library/ms190673.aspx.

Чтобы хранить данные теневого копирования в файлах на диске, снимите флажок **Хранить файлы теневого копирования в базе данных**. При этом в базе данных сервера будут храниться только указатели файлов и небольшое количество других данных о теневых копиях.

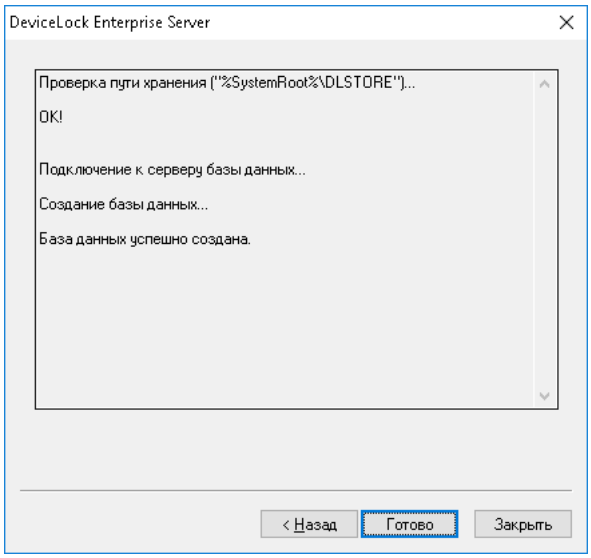
Когда данные теневого копирования хранятся в файлах на диске, сами файлы располагаются в папке, указанной в параметре **Путь к хранилищу**. Для выбора папки используйте кнопку **Обзор**. Можно выбрать папку на локальном диске или указать UNC-путь папки на файловом сервере (например, `\\server\share\folder`). Учетная запись, под которой запущена служба DeviceLock Enterprise Server, должна иметь полный доступ к этой папке.

Примечание: Мы рекомендуем хранить данные теневого копирования в файлах на диске.

Нажмите кнопку **Далее**, чтобы применить настройки и перейти к последней странице мастера.

Завершение настройки

Создание базы данных займет некоторое время. Если база данных уже существует на указанном сервере и имеет правильный формат (создана программой настройки DeviceLock), то DeviceLock Enterprise Server будет использовать эту существующую базу данных. При необходимости DeviceLock автоматически обновляет базу данных до последней версии.



На данной странице мастера можно наблюдать за применением указанных параметров базы данных и просматривать ошибки, которые могут возникнуть при ее настройке.

Если не удается создать или настроить базу данных или папку для хранения файлов теневого копирования, в диалоговом окне могут появиться следующие сообщения об ошибках:

- **[2] The system cannot find the file specified** - Выбран режим хранения данных теневого копирования в файлах на диске, но при этом параметр **Путь к хранилищу** указывает некорректный путь к папке. Если для папки указан UNC-путь, то, возможно, сетевой ресурс по этому пути недоступен.
- **Failed to verify store path. [5] Access is denied** - Параметр **Путь к хранилищу** указывает корректный путь к папке, но учетная запись, под которой запущена служба DeviceLock Enterprise Server, не обладает правом полного доступа к этой папке.
- **CREATE DATABASE permission denied in database 'name'** - У учетной записи, используемой для подключения к SQL Server, недостаточно прав для создания базы данных. Этой учетной записи требуется как минимум серверная роль **dbcreator** (см. **Server Roles** в **Login Properties** у Microsoft SQL Server Management Studio).
- **The server principal "user_name" is not able to access the database "name" under the current security context** - Учетная запись, используемая для подключения к SQL Server, не может получить доступ к существующей базе данных. Учетная запись должна быть привязана к этой базе данных (см. **User Mapping** в **Login Properties** у Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** - Учетная запись, используемая для подключения к SQL Server, не может получить доступ на чтение/запись в существующей базе данных. Учетной записи требуются как минимум роли базы данных **db_datareader** и **db_datawriter** (см. **User Mapping** в **Login Properties** у Microsoft SQL Server Management Studio).
- **Invalid object name 'name'** - База данных, указанная в параметре **Имя базы данных**, существует, но имеет неверный формат. Такая ошибка обычно возникает при попытке использовать базу данных, которая повреждена или создана программой, отличной от программы настройки DeviceLock Enterprise Server.
- **База данных DeviceLock имеет неподдерживаемый формат** - База данных, указанная в параметре **Имя базы данных**, существует, но имеет устаревший формат и не может быть обновлена до новой версии. Ее формат не удается преобразовать для использования совместно с новой версией DeviceLock. Укажите имя другой базы данных или задайте новое имя, чтобы создать новую базу данных.
- **База данных DeviceLock имеет формат, который не поддерживается текущей версией сервера** - База данных, указанная в параметре **Имя базы данных**, существует, но была создана новой версией DeviceLock Enterprise Server. Используйте новую версию DeviceLock Enterprise Server или задайте другое имя базы данных.

Помимо перечисленных выше ошибок могут появиться также некоторые ошибки, приведенные в разделе Проверка соединения ранее в этом документе.

При появлении ошибок используйте кнопку **Назад**, чтобы вернуться на предыдущую страницу и внести необходимые изменения в настройки.

При отсутствии ошибок нажмите кнопку **Готово**, чтобы закрыть мастер настройки и продолжить процесс установки.

Далее, на странице **Мастер установки завершен** нажмите кнопку **Готово**, чтобы завершить процесс установки. С завершающей страницы мастера установки можно перейти на веб-сайт DeviceLock. Этот вариант выбран по умолчанию.

Примечание: Удалить DeviceLock можно следующим образом:

- Используйте средство **Программы и компоненты** панели управления Windows (**Установка и удаление программ** на ранних версиях Windows).

  - или -
- Выберите пункт **Удалить DeviceLock** в меню **Пуск** Windows.

Установка DeviceLock Content Security Server

В данном разделе описаны шаги по установке DeviceLock Content Security Server:

1. Подготовка к установке
2. Запуск установки
3. Настройка и завершение установки

Подготовка к установке

Прежде чем приступать к установке, примите во внимание следующее:

- Программа установки DeviceLock Content Security Server устанавливает два компонента DeviceLock: поисковый сервер и сервер Discovery.
- Для установки и работы DeviceLock Content Security Server должны быть выполнены следующие требования к системе:

Операционная система	Microsoft Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016 или Windows Server 2019. Допускаются 32- и 64-разрядные версии операционной системы.
Сервер базы данных	Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014, 2016, 2017 или 2019, любой выпуск, в том числе SQL Server Express. **Внимание:** Сервер базы данных необходим для работы поискового сервера и сервера Discovery (см. Настройка базы данных).
Свободное место на жестком диске	Минимум: 1 ГБ Рекомендуется: 800 ГБ (в случае локального сервера базы данных)

- Для установки DeviceLock Content Security Server требуются права локального администратора.
- В целях наилучшей производительности и надежности рекомендуется устанавливать серверы DeviceLock Enterprise Server и DeviceLock Content Security Server на разных компьютерах.

- Для поискового сервера необходимо приобрести специальную лицензию. Одну и ту же лицензию можно установить на любом количестве компьютеров, на которых работает DeviceLock Content Security Server.

  Лицензирование поискового сервера основано на количестве записей в журналах, которые будут индексироваться для полнотекстового поиска. Каждая лицензия позволяет индексировать 1 000 записей в журнале теневого копирования (включая теневые копии документов), 1 000 записей в журнале активности пользователей (включая записи ввода с клавиатуры) и по 5 000 записей в каждом из прочих журналов (журнал аудита, журнал удаленных данных теневого копирования, журнал сервера, журнал мониторинга и журнал политик).

  Требуемое количество лицензий поискового сервера зависит от количества записей в журналах сервера DeviceLock Enterprise Server. Максимально возможное количество индексируемых записей вычисляется исходя из общего числа установленных лицензий. При необходимости можно в любое время приобрести и установить дополнительные лицензии.

  Пробный период для сервера DeviceLock Content Security Server составляет 30 дней. В течение этого периода сервер может индексировать 2 000 записей в журнале теневого копирования, 2 000 записей в журнале активности пользователей и по 10 000 записей в каждом из прочих журналов.

- Для сервера Discovery необходимо приобрести специальную лицензию на DeviceLock Discovery. Лицензия требуется для каждого компьютера или сетевого ресурса, который требуется сканировать с помощью DeviceLock Discovery, независимо от того, сканируется весь компьютер или только отдельная папка. Период пробной эксплуатации DeviceLock Discovery составляет 30 дней. В течение этого периода можно сканировать не более двух компьютеров или сетевых ресурсов.

- Если в сети имеется несколько экземпляров DeviceLock Enterprise Server, то для распределения нагрузки можно также установить несколько экземпляров DeviceLock Content Security Server.

- Если установлено несколько экземпляров DeviceLock Content Security Server, каждый из них будет использовать собственный индекс для поиска. Следовательно, чтобы получить полный набор результатов поиска по всем данным, хранящимся на всех экземплярах DeviceLock Enterprise Server, понадобится выполнить одинаковые поисковые запросы на каждом экземпляре DeviceLock Content Security Server.

- Предусмотрены два варианта сопряжения сервера DeviceLock Content Security Server и сервера базы банных. Перед установкой DeviceLock Content Security Server выберите подходящий для вас вариант:

  1. ОДИН К ОДНОМУ - Устанавливается один сервер DeviceLock Content Security Server с подключением к одному серверу базы данных. Этот вариант подходит для небольших сетей (до нескольких сотен компьютеров).

  2. МНОГИЕ КО МНОГИМ - Устанавливаются нескольких серверов DeviceLock Content Security Server с подключением каждого к индивидуальному серверу базы данных. Этот вариант подходит для средних и крупных сетей, географически разделенных на несколько сегментов.

- Перед запуском программы установки следует закрыть все приложения, ранее запущенные в Windows.

Запуск установки

Используйте следующую процедуру для начала процесса установки.

Чтобы начать установку

1. Откройте архив `DeviceLock.zip`, а затем дважды щелкните файл `setup_dlcss.exe`, чтобы запустить программу установки.

   Программу установки нужно запускать на каждом компьютере, где требуется установить DeviceLock Content Security Server.

2. Следуйте инструкциям в программе установки.
3. На странице **Лицензионное соглашение** ознакомьтесь с лицензионным соглашением и нажмите кнопку **Я принимаю условия лицензионного соглашения**, чтобы принять условия лицензионного соглашения и продолжить установку.
4. На странице **Сведения о пользователе** введите свое имя и название организации и нажмите кнопку **Далее**.
5. На странице **Папка назначения** примите папку установки по умолчанию или нажмите кнопку **Изменить**, чтобы выбрать другую папку. Нажмите кнопку **Далее**.

   Папка установки по умолчанию - `%ProgramFiles%\DeviceLock Content Security Server` на 32-битной Windows или `%ProgramFiles(x86)%\DeviceLock Content Security Server` на 64-битной.

6. На странице **Система готова к установке программы** нажмите кнопку **Установить**, чтобы начать установку.

   Появится мастер настройки DeviceLock Content Security Server.

   Если вы устанавливаете обновление DeviceLock Content Security Server или переустанавливаете его и не хотите ничего менять в текущих настройках, нажмите кнопку **Далее**, и затем нажмите кнопку **Отмена**, чтобы закрыть мастер настройки.

   Если требуется изменить какие-либо параметры, сохраняя все остальные настройки, измените только необходимые параметры, пройдите через все страницы мастера настройки и нажмите кнопку **Готово** на последней странице.

   Примечание: Если вы устанавливаете Content Security Server в первый раз на данный компьютер и при этом закрываете мастер настройки, не задав параметры запуска службы DeviceLock Content Security Server, программа установки не сможет настроить эту службу, и будет снова предложено использовать мастер настройки.

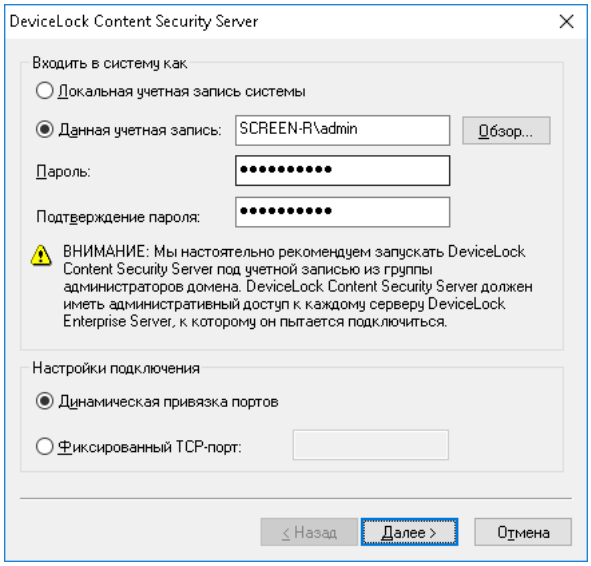
Настройка и завершение установки

Мастер настройки запускается автоматически в процессе установки и предоставляет следующие страницы для настройки DeviceLock Content Security Server:

- Учетная запись службы и параметры подключения
- Администраторы сервера и сертификат
- Информация о лицензии
- Настройка базы данных
- Завершение настройки

Учетная запись службы и параметры подключения

На первой странице мастера настройки задается учетная запись запуска службы DeviceLock Content Security Server и выбирается TCP-порт для подключения к этому серверу.



Входить в систему как

Необходимо задать учетную запись для запуска службы DeviceLock Content Security Server. Это может быть локальная учетная запись системы или другая учетная запись.

Для запуска службы под учетной записью системы, выберите опцию **Локальная учетная запись системы**. Следует помнить, что программы, работающие под этой учетной записью, не могут получить доступ к сетевым ресурсам и авторизуются на удаленных компьютерах как анонимный непривилегированный пользователь. Таким образом, DeviceLock Content Security Server, запущенный под локальной учетной записью системы, не сможет получить доступ к сетевым ресурсам, и должен будет использовать сертификат DeviceLock для авторизации на сервере DeviceLock Enterprise Server, работающем на удаленном компьютере.

Дополнительную информацию о методах авторизации можно найти в описании параметра Имя сертификата.

Внимание: Если служба DeviceLock Content Security Server запускается под учетной записью системы, то сервер Discovery не сможет устанавливать и удалять агенты Discovery на удаленных компьютерах.

Для запуска службы под другой учетной записью выберите опцию **Данная учетная запись** и введите имя пользователя и его пароль. Рекомендуется использовать учетную запись пользователя с правами администратора на всех компьютерах, где работает сервер DeviceLock Enterprise Server. В противном случае для авторизации потребуется использовать сертификат DeviceLock.

При установке DeviceLock Content Security Server в домене Active Directory для запуска службы рекомендуется использовать учетную запись, включенную в группу администраторов домена (Domain Admins). В результате служба получит права администратора на всех компьютерах данного домена, поскольку группа администраторов домена по умолчанию входит в локальную группу администраторов на каждом компьютере, подключенном к домену.

Необходимо также учитывать следующие соображения:

- Если на удаленном сервере DeviceLock Enterprise Server не используется режим безопасности по умолчанию (снят флажок **Включить безопасность по умолчанию**), то на таком сервере учетная запись, указанная в параметре **Данная учетная запись**, должна быть в списке администраторов с уровнем доступа как минимум **Только чтение**. В противном случае для авторизации потребуется использовать сертификат DeviceLock.
- Если на удаленном сервисе DeviceLock не используется режим безопасности по умолчанию (снят флажок **Включить безопасность по умолчанию**), то на таком сервисе учетная запись, указанная в параметре **Данная учетная запись**, должна быть в списке администраторов DeviceLock с уровнем доступа как минимум **Только чтение**. В противном случае потребуется использовать авторизацию по сертификату DeviceLock или задать имя и пароль альтернативной учетной записи для соответствующего подразделения DeviceLock Discovery.

Настройки подключения

DeviceLock Content Security Server можно настроить на использование определенного TCP-порта для связи с консолью управления: выберите опцию **Фиксированный TCP-порт** и введите номер порта. Для автоматического выбора порта выберите опцию **Динамическая привязка портов**. По умолчанию DeviceLock Content Security Server использует порт 9134.

Нажмите кнопку **Далее**, чтобы запустить службу DeviceLock Content Security Server и перейти на вторую страницу мастера.

Запуск службы DeviceLock Content Security Server

Если пользователь, запустивший мастер настройки, не является администратором DeviceLock Content Security Server (в ситуации, когда устанавливается обновление поверх уже настроенного сервера), мастер настройки не сможет установить службу сервера и внести изменения в его параметры. Появится следующее сообщение: “Доступ запрещен.” Та же ошибка может возникнуть, если этот пользователь не обладает правами администратора на компьютере, где выполняется установка DeviceLock Content Security Server.

Если для параметра **Данная учетная запись** указано несуществующее имя пользователя или неправильно введен пароль, то операционная система не сможет запустить службу DeviceLock Content Security Server. Появится следующее сообщение: “Имя учетной записи задано неверно или не существует, или же неверен указанный пароль.”

Если учетная запись, указанная в параметре **Данная учетная запись**, не является членом группы администраторов домена (Domain Admins), появится следующее сообщение: “Учетная запись <имя> не принадлежит к группе администраторов домена. Вы хотите продолжить?”

Можно продолжить, нажав кнопку **Да**. При этом должны быть выполнены перечисленные ниже требования.

Для поискового сервера:

- Указанная учетная запись должна обладать правами администратора на всех удаленных компьютерах, на которых работает DeviceLock Enterprise Server.

  - или -

- Секретный ключ сертификата DeviceLock должен быть установлен на каждом компьютере, где работает DeviceLock Enterprise Server.

Для сервера Discovery:

- Указанная учетная запись должна обладать правами администратора на всех компьютерах, сканируемых сервером Discovery. Это компьютеры, на которых работает сервис DeviceLock или агент Discovery, а также компьютеры, сканирование которых будет производиться без использования агентов.

  - или -

- Открытый ключ сертификата DeviceLock должен быть установлен на каждом компьютере (с установленным сервисом DeviceLock), который подлежит сканированию сервером Discovery.

  - или -

- Данные альтернативной учетной записи (имя пользователя и пароль) должны быть заданы в настройках сканирования.

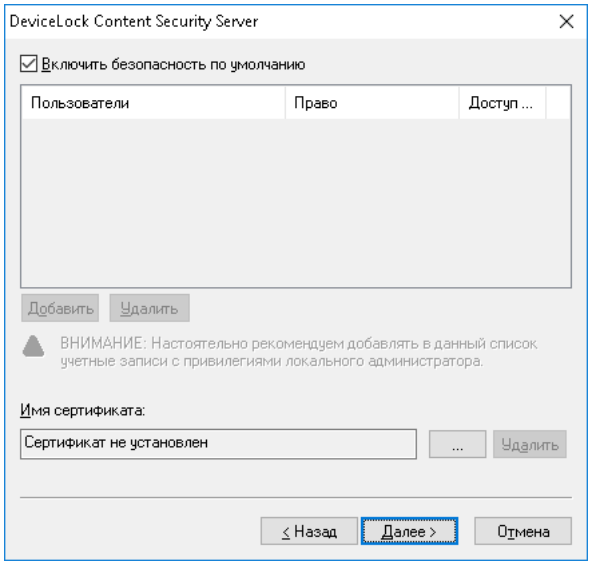
Если учетная запись, указанная для параметра **Данная учетная запись**, не обладает системной привилегией “Входить в систему как служба”, мастер настройки автоматически присвоит ей эту привилегию. Данная привилегия необходима для запуска службы под учетной записью пользователя. Появится следующее сообщение: “Для учетной записи <имя> добавлено право входить в систему как служба.”

Если параметры запуска заданы верно, выполняется запуск службы. Появляется следующее сообщение: “Пожалуйста, подождите, пока программа взаимодействует со службой. Запуск службы DLCSS на компьютере: Локальный компьютер…”

Запуск службы DeviceLock Content Security Server занимает некоторое время (около минуты), после чего отображается вторая страница мастера настройки.

Администраторы сервера и сертификат

На второй странице мастера можно задать список администраторов сервера DeviceLock Content Security Server, а также установить секретный ключ сертификата DeviceLock.



Включить безопасность по умолчанию

При контроле доступа к DeviceLock Content Security Server по умолчанию любые пользователи, обладающие правами локального администратора, могут подключаться к DeviceLock Content Security Server с помощью консоли управления, изменять его настройки, выполнять поисковые запросы и запускать задачи сканирования и обнаружения.

Чтобы включить контроль доступа по умолчанию, установите флажок **Включить безопасность по умолчанию**.

Если требуется более гибкий контроль доступа к DeviceLock Content Security Server, отключите контроль по умолчанию, сняв флажок **Включить безопасность по умолчанию**.

Если флажок **Включить безопасность по умолчанию** снят, нужно задать список учетных записей (пользователей и/или групп), которые смогут подключаться к DeviceLock Content Security Server. Чтобы добавить учетную запись в этот список, нажмите кнопку **Добавить**. Можно добавить несколько учетных записей одновременно.

Для удаления учетных записей из списка используйте кнопку **Удалить**. Используя клавиши Ctrl и/или Shift, можно выбрать и удалить несколько записей одновременно.

Чтобы установить, какие действия разрешены пользователю или группе, выберите желаемый уровень доступа к серверу:

- **Полный доступ** - Позволяет устанавливать и удалять сервер DeviceLock Content Security Server, подключаться к нему с помощью консоли DeviceLock Management Console и выполнять любые действия на сервере, в том числе: просматривать и изменять настройки сервера; создавать и запускать поисковые запросы и задачи; просматривать и изменять настройки обнаружения контента; создавать и запускать задачи и отчеты обнаружения контента.
- **Изменение** - То же, что и полный доступ к серверу, за исключением права вносить изменения в список администраторов сервера, а также права изменять уровень доступа к серверу для пользователей и групп, уже имеющихся в этом списке.
- **Только чтение** - Позволяет подключаться к серверу DeviceLock Content Security Server с помощью консоли DeviceLock Management Console, просматривать настройки сервера, выполнять поисковые запросы, просматривать и запускать уже имеющиеся поисковые задачи, просматривать настройки обнаружения контента, а также просматривать отчеты по результатам сканирования и обнаружения и вручную создавать новые отчеты на основе существующих отчетов и данных, подготовленных задачами сканирования и обнаружения контента. Не позволяет запускать такие задачи, вносить какие-либо изменения на сервере, или создавать новый индекс для поискового сервера.

Для пользователей и групп с уровнем доступа **Изменение** или **Только чтение** можно выбрать опцию **Доступ к теневым копиям**, чтобы обеспечить доступ к теневым копиям и записям активности пользователей. Пользователи и группы, для которых выбрана эта опция, могут выполнять поиск по содержимому теневых копий и записей активности пользователей, а также открывать, просматривать и сохранять теневые копии и записи активности пользователей, обнаруженные в результате поиска.

Администраторы сервера DeviceLock Content Security Server, у которых нет доступа к теневым копиям, не могут открывать, просматривать и сохранять теневые копии и записи активности пользователей. На результатах поиска нет ссылок **Открыть**, **Сохранить** и **Просмотр**, а вместо текстовых фрагментов теневых копий и записей активности пользователей отображаются звездочки. Логины и пароли в параметрах документа для записей активности пользователей также заменяются звездочками.

Внимание: Настоятельно рекомендуется предоставить администраторам сервера права локального администратора, поскольку при установке, обновлении или удалении сервера DeviceLock Content Security Server может потребоваться доступ к диспетчеру служб Windows (Service Control Manager) и общим сетевым ресурсам.

Имя сертификата

Чтобы использовать авторизацию на основе сертификата DeviceLock, на DeviceLock Content Security Server нужно установить секретный ключ этого сертификата.

Предусмотрены два метода авторизации поискового сервера на сервере DeviceLock Enterprise Server, работающем на удаленном компьютере:

- **Авторизация по пользователю** - Служба DeviceLock Content Security Server запущена под учетной записью, обладающей правами администратора DeviceLock Enterprise Server на удаленном компьютере. Инструкции по выбору учетной записи для запуска службы DeviceLock Content Security Server см. в описании параметра Входить в систему как.
- **Авторизация по сертификату** - Если учетная запись, используемая для запуска службы DeviceLock Content Security Server, не обладает правами администратора DeviceLock Enterprise Server на удаленном компьютере, необходимо использовать авторизацию на основе сертификата DeviceLock.

  Для авторизации по сертификату нужно установить один и тот же секретный ключ сертификата DeviceLock как на DeviceLock Enterprise Server, так и на DeviceLock Content Security Server.

Предусмотрены три метода авторизации сервера Discovery на сканируемых компьютерах:

- **Авторизация по пользователю** - Служба DeviceLock Content Security Server запущена под учетной записью, которая будет использована при сканировании удаленных компьютеров. Данная учетная запись будет также использована для подключения либо к сервису DeviceLock, либо к агенту Discovery, или же для подключения к удаленному компьютеру, сканирование которого будет производиться без использования агента. Инструкции по выбору учетной записи для запуска службы DeviceLock Content Security Server см. в описании параметра Входить в систему как.
- **Авторизация под другим пользователем** - Служба DeviceLock Content Security Server запущена под учетной записью, обладающей правами администратора по крайней мере на локальном компьютере. Сервер Discovery будет использовать альтернативную учетную запись для доступа к удаленному компьютеру в процессе сканировании.
- **Авторизация по сертификату** - Метод, использующий сертификат для авторизации на удаленных компьютерах, на которых запущен сервис DeviceLock и установлен соответствующий открытый ключ сертификата.

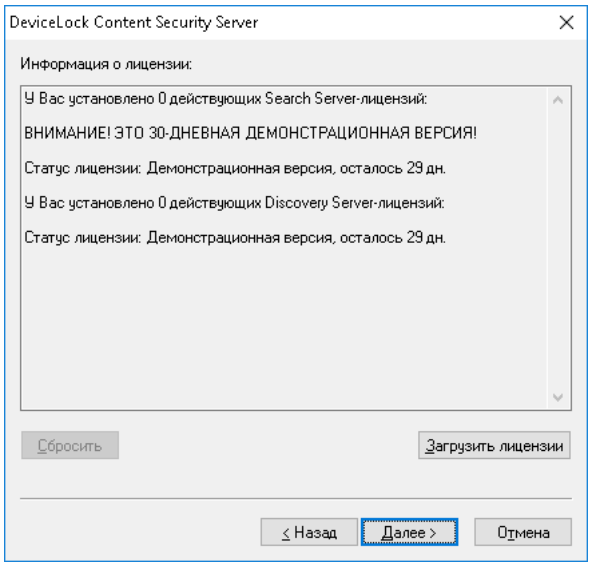
Подробнее о сертификатах см. в разделе Сертификаты DeviceLock данного руководства.

Чтобы установить сертификат, нажмите кнопку ... и выберите файл с секретным ключом. Чтобы удалить сертификат, нажмите кнопку **Удалить**.

Нажмите кнопку **Далее**, чтобы применить настройки и перейти к следующей странице мастера настройки.

Информация о лицензии

Данная страница служит для установки лицензий на поисковый сервер (Search Server-лицензий) и/или на сервер Discovery (Discovery Server-лицензий). На каждый из этих серверов требуется отдельная лицензия. Период пробной эксплуатации составляет 30 дней.



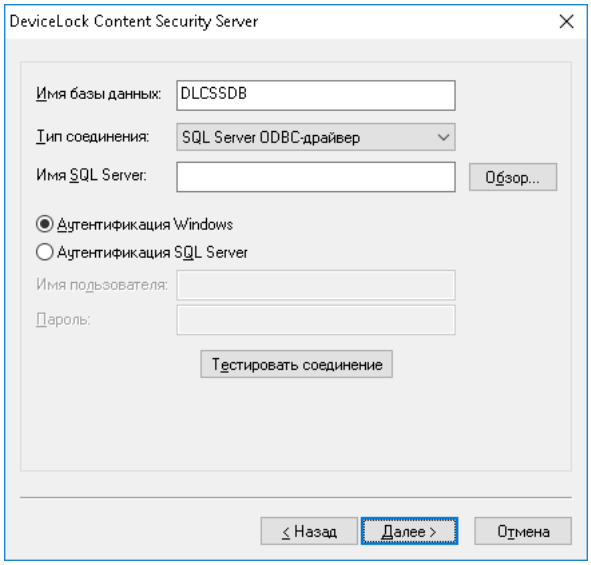
Чтобы установить лицензию, нажмите кнопку **Загрузить лицензии** и выберите файл с лицензией. Можно загрузить несколько файлов подряд - один за другим. В окне **Информация о лицензии** отображается сводная информация об устанавливаемых вами лицензиях.

После установки DeviceLock Content Security Server можно использовать консоль DeviceLock Management Console для установки лицензии или просмотра текущей информации о лицензии, включая количество установленных лицензий и количество используемых лицензий для поискового сервера и/или сервера Discovery.

Нажмите кнопку **Далее,** чтобы перейти к настройке базы данных.

Настройка базы данных

Следующая страница используется для настройки базы данных сервера DeviceLock Content Security Server.



Внимание: Не пропускайте эту страницу мастера, поскольку база данных необходима для работы поискового сервера и сервера Discovery. При отсутствии базы данных невозможен поиск с использованием контентно-зависимых групп, сохранение и автоматизация поисковых запросов, а также сканирование и обнаружение контента при помощи сервера Discovery.

Имя базы данных

В поле **Имя базы данных** укажите имя базы данных для сервера DeviceLock Content Security Server. Мастер настройки по умолчанию предлагает имя **DLCSSDB**.

Примечание: Не следует вручную создавать базу данных с указанным именем; мастер настройки сам создает базу данных или использует уже существующую.

Тип соединения

В списке **Тип соединения** можно выбрать подходящий вариант соединения с базой данных. Предусмотрены следующие варианты:

- **SQL Server ODBC-драйвер** - Подключение к серверу Microsoft SQL Server с помощью драйвера ODBC.

  В параметре **Имя SQL Server** указывается имя, обычно содержащее две части: короткое имя компьютера, за которым следует имя экземпляра SQL Server, отделенное обратной косой чертой (например, `computer\instance`). Для экземпляра по умолчанию в качестве имени SQL Server используется короткое имя компьютера (имя экземпляра отсутствует).

  Чтобы получить имена серверов SQL Server, доступных в локальной сети, нажмите кнопку **Обзор**. Для получения имени сервера требуется удаленный доступ к реестру компьютера, на котором работает SQL Server.

  Если параметр **Имя SQL Server** не задан, то считается, что выбран экземпляр SQL Server по умолчанию, работающий компьютере, на котором установлен DeviceLock Content Security Server.

Для доступа к SQL Server необходимо настроить параметры аутентификации.

Выберите опцию **Аутентификация Windows** для доступа к SQL Server от имени учетной записи, под которой запущена служба DeviceLock Content Security Server.

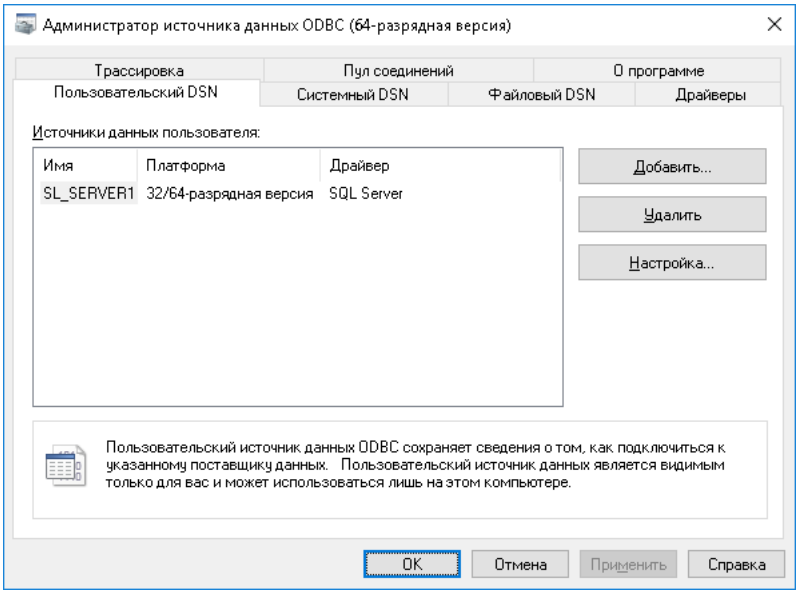
Если служба запущена под локальной учетной записью системы, а SQL Server находится на другом компьютере, DeviceLock Content Security Server не сможет получить доступ к SQL Server, т.к. локальная учетная запись системы не имеет права на доступ к сетевым ресурсам. Подробнее о выборе учетной записи для службы DeviceLock Content Security Server см. в описании параметра Входить в систему как.

Выберите опцию **Аутентификация SQL Server** для доступа к SQL Server от имени заданного пользователя SQL Server. Прежде чем выбрать эту опцию, убедитесь, что SQL Server был настроен для работы в смешанном режиме аутентификации. Укажите имя пользователя SQL Server в параметре **Имя пользователя** и соответствующий ему пароль в параметре **Пароль**.

Примечание: Аутентификация Windows обеспечивает более высокий уровень безопасности по сравнению с аутентификацией SQL Server, так что по возможности следует использовать аутентификацию Windows.

- **Системный источник данных** - Подключение к серверу базы данных с помощью ранее созданного системного источника данных. Выберите источник данных из списка **Имя источника данных**.

  Чтобы создать источник данных, используйте компонент **Администратор источника данных ODBC** в разделе **Панель управления** > **Администрирование**.



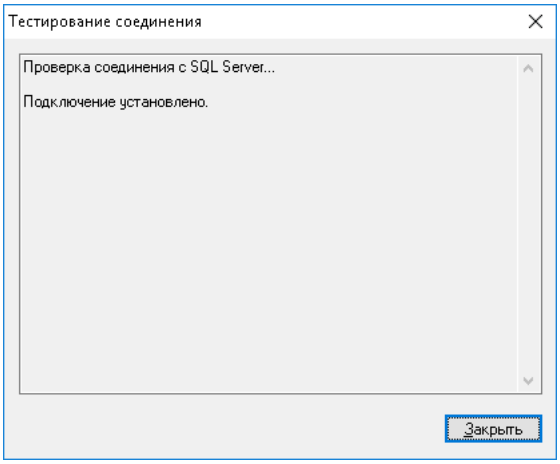
Если источник данных требует имя пользователя и пароль (например, в случае режима аутентификации SQL Server), необходимо указать имя пользователя и его пароль в поле **Имя пользователя** и **Пароль**, соответственно. В противном случае оставьте пустыми оба эти поля.

Чтобы обновить список **Имя источника данных**, нажмите кнопку **Обновить**.

Проверка соединения

Задав параметры соединения, можно выполнить проверку, чтобы убедиться в их корректности. Для этого нажмите кнопку **Тестировать соединение**.

Проверяется только соединение с сервером базы данных. В случае успешного подключения к серверу диалоговое окно **Тестирование соединения** не покажет никаких ошибок, даже при наличии каких-либо проблем с базой данных или доступом к ней.



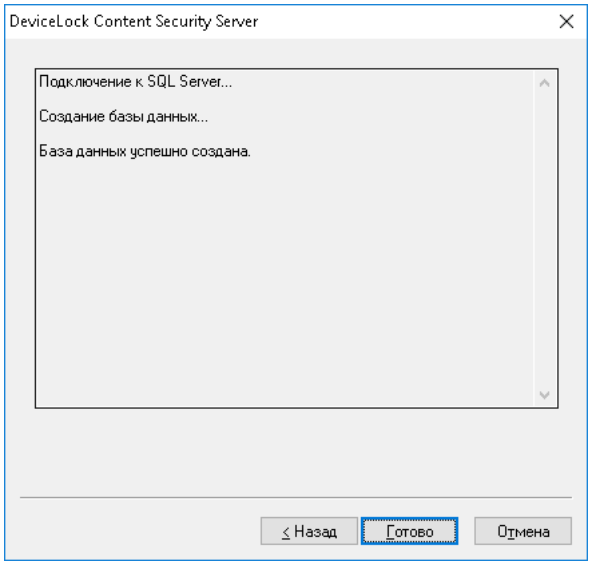
Если не удается установить соединение с использованием заданных параметров, в диалоговом окне могут появиться следующие сообщения об ошибках:

- **SQL Server does not exist or access denied** - Указано неправильное имя в параметре **Имя SQL Server**, либо компьютер, на котором работает SQL Server, недоступен. Возможно, указано имя компьютера, но не указано имя экземпляра SQL Server (имя нужно указывать в формате computer\instance).
- **Login failed for user 'COMPUTER_NAME$'** - Выбран режим аутентификации Windows, но учетная запись, под которой запущена служба DeviceLock Content Security Server, не может получить доступ к SQL Server. Возможно служба запущена под локальной учетной записью системы или под учетной записью, не обладающей правами администратора на компьютере SQL Server.
- **Login failed for user 'user_name'** - Выбран режим аутентификации SQL Server, но неверно задано имя пользователя SQL Server (логин) или его пароль. В параметре **Имя пользователя** должно быть указано имя пользователя SQL Server, а не пользователя Windows. Для администрирования пользователей SQL Server используются средства SQL Server (такие как Microsoft SQL Server Management Studio).
- **Login failed for user 'user_name'. The user is not associated with a trusted SQL Server connection** - Выбран режим аутентификации SQL Server, но SQL Server не поддерживает данный режим. Необходимо либо использовать режим аутентификации Windows, либо настроить SQL Server для работы в смешанном режиме аутентификации.
- **Login failed for user ''. The user is not associated with a trusted SQL Server connection** - Источник данных, указанный в параметре **Имя источника данных** настроен для работы в режиме аутентификации SQL Server, но параметр **Имя пользователя** не задан.
- **Data source name not found and no default driver specified** - Задано неправильное значение параметра **Имя источника данных** (например, пустая строка).

Нажмите кнопку **Далее**, чтобы применить настройки и перейти к последней странице.

Завершение настройки

Создание базы данных займет некоторое время. Если база данных уже существует на указанном сервере и имеет правильный формат (создана программой настройки DeviceLock), то DeviceLock Content Security Server будет использовать эту существующую базу данных. При необходимости DeviceLock автоматически обновляет базу данных до последней версии.



На данной странице мастера можно наблюдать за применением указанных параметров базы данных и просматривать ошибки, которые могут возникнуть при ее настройке.

Если не удается создать или настроить базу данных с использованием заданных параметров, в диалоговом окне могут появиться следующие сообщения об ошибках:

- **CREATE DATABASE permission denied in database 'name'** - У учетной записи, используемой для подключения к SQL Server, недостаточно прав для создания базы данных. Этой учетной записи требуется как минимум серверная роль **dbcreator** (см. **Server Roles** в **Login Properties** у Microsoft SQL Server Management Studio).
- **The server principal "user_name" is not able to access the database "name" under the current security context** - Учетная запись, используемая для подключения к SQL Server, не может получить доступ к существующей базе данных. Учетная запись должна быть привязана к этой базе данных (см. **User Mapping** в **Login Properties** у Microsoft SQL Server Management Studio).
- **SELECT permission denied on object 'name', database 'name', schema 'name'** - Учетная запись, используемая для подключения к SQL Server, не может получить доступ на чтение/запись в существующей базе данных. Учетной записи требуются как минимум роли базы данных **db_datareader** и **db_datawriter** (см. **User Mapping** в **Login Properties** у Microsoft SQL Server Management Studio).
- **Invalid object name 'name'** - База данных, указанная в параметре **Имя базы данных**, существует на SQL Server, но имеет неверный формат. Такая ошибка обычно возникает при попытке использовать базу данных, которая повреждена или создана программой, отличной от программы настройки DeviceLock Content Security Server.
- **DeviceLock Database has an unsupported format** - База данных, указанная в параметре **Имя базы данных**, существует на SQL Server, но имеет устаревший формат и не может быть обновлена до новой версии. Ее формат не удается преобразовать для использования совместно с новой версией DeviceLock. Укажите имя другой базы данных или задайте новое имя, чтобы создать новую базу данных.

- **DeviceLock Database has a format that is not supported by the current server version** - База данных, указанная в параметре **Имя базы данных**, существует на SQL Server, но она была создана новой версией DeviceLock Content Security Server. Используйте новую версию DeviceLock Content Security Server или задайте другое имя базы данных.

Помимо перечисленных выше ошибок могут появиться также некоторые ошибки, приведенные в разделе Проверка соединения ранее в этом документе.

При появлении ошибок нажмите кнопку **Назад**, чтобы вернуться на предыдущую страницу и внести необходимые изменения в настройки.

При отсутствии ошибок нажмите кнопку **Готово**, чтобы закрыть мастер настройки и продолжить процесс установки.

Далее, на странице **Мастер установки завершен** нажмите кнопку **Готово**, чтобы завершить процесс установки. С этой страницы можно перейти на веб-сайт DeviceLock. Этот вариант выбран по умолчанию.

Примечание: Удалить DeviceLock Content Security Server можно следующим образом:

- Используйте средство **Программы и компоненты** панели управления Windows (**Установка и удаление программ** на ранних версиях Windows).

  - или -
- Выберите пункт **Удалить DeviceLock Content Security Server** в меню **Пуск** Windows.

3

Консоли и инструменты DeviceLock

В этой главе:

DeviceLock Management Console

DeviceLock Service Settings Editor

DeviceLock Group Policy Manager

DeviceLock Enterprise Manager

Сертификаты DeviceLock

Мастер создания подписи

DeviceLock Management Console

Консоль DeviceLock Management Console - это оснастка для Microsoft Management Console (MMC).

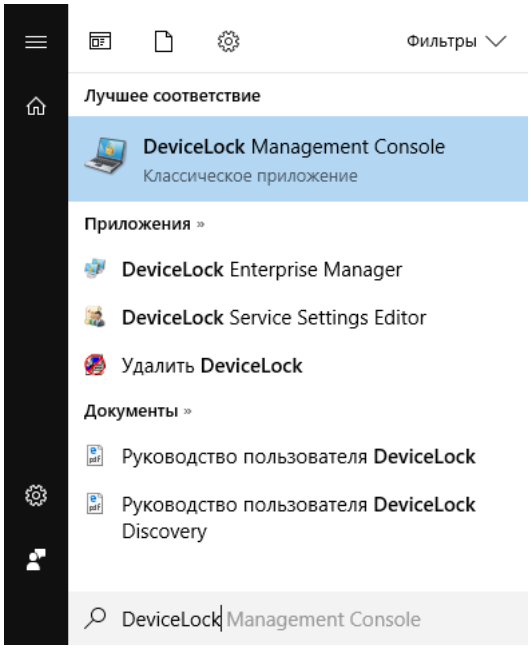
С помощью консоли DeviceLock Management Console можно просматривать и изменять разрешения и правила аудита, устанавливать сервис DeviceLock, а также просматривать журналы аудита и теневого копирования для отдельных компьютеров.

Консоль DeviceLock Management Console также используется для просмотра журналов, хранящихся на сервере DeviceLock Enterprise Server, выполнения поисковых запросов на сервере DeviceLock Content Security Server и управления этими серверами.

Консоль DeviceLock Management Console необходимо использовать на компьютере, с которого будет осуществляться управление экземплярами сервиса DeviceLock и серверами DeviceLock Enterprise Server и DeviceLock Content Security Server, находящимися в сети.

Инструкции по установке консоли DeviceLock Management Console можно найти в разделе Установка консолей управления данного руководства.

Открыть консоль можно, запустив приложение DeviceLock Management Console со стартовой страницы Windows.

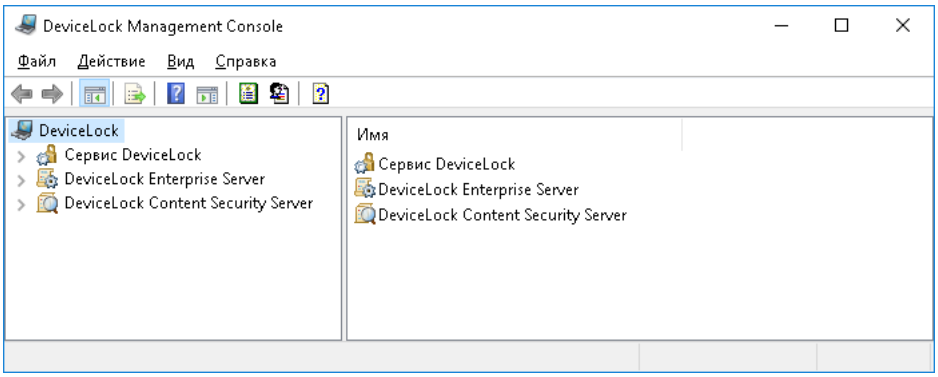


Кроме того, можно запустить MMC и добавить оснастку DeviceLock Management Console вручную:

1. Запустите **mmc** из командной строки или используйте диалоговое окно **Выполнить** для выполнения этой команды.
2. Из меню **Файл** выберите команду **Добавить или удалить оснастку**.
3. Выберите из списка оснастку **DeviceLock Management Console** и нажмите кнопку **Добавить**.
4. Нажмите **OK**.

Пользовательский интерфейс

Консоль DeviceLock Management Console имеет дружественный, удобный в использовании интерфейс, предоставляемый Microsoft Management Console (MMC). В любом окне программы доступна контекстная справка по нажатию клавиши F1.



Консоль DeviceLock Management Console представляет собой окно, разделенное на две панели. На левой панели находится дерево консоли; на панели сведений в правой части окна отображается детальная информация. Если в дереве консоли выбран какой-либо элемент, то панель сведений отображает его содержимое.

Консоль DeviceLock Management Console содержит три независимых раздела:

1. **Сервис DeviceLock** - Позволяет подключаться и управлять сервисом DeviceLock, работающим на локальном или удаленном компьютере.
2. **DeviceLock Enterprise Server** - Позволяет подключаться и управлять сервером DeviceLock Enterprise Server, работающим на локальном или удаленном компьютере.
3. **DeviceLock Content Security Server** - Позволяет подключаться и управлять сервером DeviceLock Content Security Server, работающим на локальном или удаленном компьютере.

Узел "DeviceLock" в корне дерева консоли

Этот корневой узел представляет DeviceLock в консоли управления.

Контекстное меню узла **DeviceLock** в дереве консоли DeviceLock Management Console содержит следующие команды:

- **Мастер создания сертификата** - Запускает программу для создания сертификатов DeviceLock. Подробнее см. в разделе Создание сертификата.
- **Мастер создания подписи** - Запускает программу для авторизации устройств во временном белом списке и подписывания файлов с настройками сервиса DeviceLock. Подробнее см. в разделе Мастер создания подписи.
- **О программе DeviceLock** - Отображает диалоговое окно с информацией о версии и установленных лицензиях на DeviceLock.

В дополнение к этим командам контекстное меню узла **Настройки DeviceLock** в консоли DeviceLock Service Settings Editor или **DeviceLock** в консоли DeviceLock Group Policy Manager содержит следующие команды:

- **Сбросить всю политику в неопределенное состояние** - Устанавливает все параметры в состояние "не задано". Эта команда имеет такой же эффект, как и последовательный сброс параметров по одному.
- **Сбросить политику ContentLock в неопределенное состояние** - Сбрасывает все настройки ContentLock (все правила работы с контентом, кроме тех, которые основаны на типах файлов) в состояние "не задано".
- **Сбросить политику NetworkLock в неопределенное состояние** - Сбрасывает все настройки NetworkLock в состояние "не задано".
- **Удалить политику ContentLock** - Полностью удаляет все настройки ContentLock (все правила работы с контентом, кроме тех, которые основаны на типах файлов). Эта команда доступна только в консоли DeviceLock Service Settings Editor.
- **Удалить политику NetworkLock** - Полностью удаляет все настройки NetworkLock. Эта команда доступна только в консоли DeviceLock Service Settings Editor.
- **Показывать политику для Windows** - Включает в консоли отображение настроек, доступных только для сервиса DeviceLock для Windows.
- **Показывать политику для Mac** - Включает в консоли отображение настроек, доступных только для сервиса DeviceLock для Mac.
- **Загрузить настройки сервиса** - Вагружает настройки из файла настроек сервиса DeviceLock. Необходимо выбрать файл, созданный путем сохранения настроек сервиса DeviceLock в одной из консолей управления (например, DeviceLock Service Settings Editor, DeviceLock Management Console или DeviceLock Group Policy Manager).

- **Сохранить настройки сервиса** - Сохраняет текущие настройки сервиса DeviceLock в файл настроек. Позже этот файл может быть загружен в консоли DeviceLock Management Console, DeviceLock Group Policy Manager и/или DeviceLock Service Settings Editor. Также файл настроек может быть отправлен пользователям, чьи компьютеры не подключены к сети и находятся вне досягаемости консолей управления. Во избежание вмешательства в файл настроек следует подписать его, используя для этого Мастер создания подписи. См. также Варианты сохранения файла настроек.
- **Сохранить и подписать настройки сервиса** - Сохраняет текущие настройки сервиса DeviceLock в файл настроек и подписывает его с помощью закрытого ключа последнего используемого сертификата DeviceLock. Эта команда меню недоступна, если в мастере создания подписи ранее не использовался закрытый ключ сертификата DeviceLock. См. также Варианты сохранения файла настроек.
- **Создать MSI-пакет** - Создает MSI-пакет для установки сервиса DeviceLock с настройками, идентичными текущим настройкам сервиса DeviceLock.

  При использовании этой команды вначале выбирается исходный MSI-пакет сервиса DeviceLock. Это может быть один из MSI-пакетов, которые поставляются вместе с DeviceLock (файлы `DeviceLock Service.msi` и `DeviceLock Service x64.msi`).

  Затем требуется указать имя результирующего MSI-пакета, который будет создан на основе исходного MSI пакета и текущих настроек сервиса DeviceLock.

  С помощью такого MSI-пакета сервис DeviceLock с уже определенными политиками безопасности (настройками) можно будет установить на удаленные компьютеры (см. Установка через групповые политики).

  Примечание: При использовании MSI-пакета для развертывания сервиса DeviceLock с помощью групповой политики настройки сервиса, заданные в этом пакете, не применяются на клиентских компьютерах при любом из следующих условий:
  - На удаленном сервисе DeviceLock выключена безопасность по умолчанию.
  - В объекте групповой политики, применяемом к клиентским компьютерам, включен параметр DeviceLock **Подавлять локальную политику**.

  Имейте в виду, что команда контекстного меню **Создать MSI-пакет** недоступна, если Microsoft Windows Installer (версии 1.0 или более поздней) не установлен на локальном компьютере.

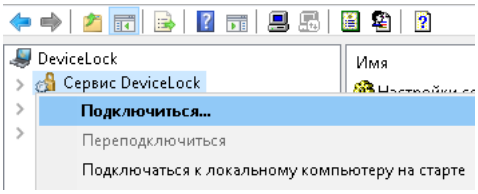
Узел “Сервис DeviceLock”

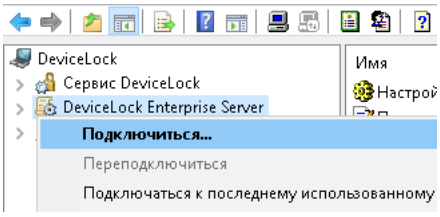
Контекстное меню узла **Сервис DeviceLock** зависит от используемой консоли:

- В консоли DeviceLock Management Console меню содержит команды для управления сервисом DeviceLock, к которому подключена консоль. Подробнее см. в разделе Управление сервисом DeviceLock для Windows.
- В консоли DeviceLock Service Settings Editor меню содержит те же команды, что и меню корневого узла (см. Узел “DeviceLock” в корне дерева консоли).

Подключение к компьютеру

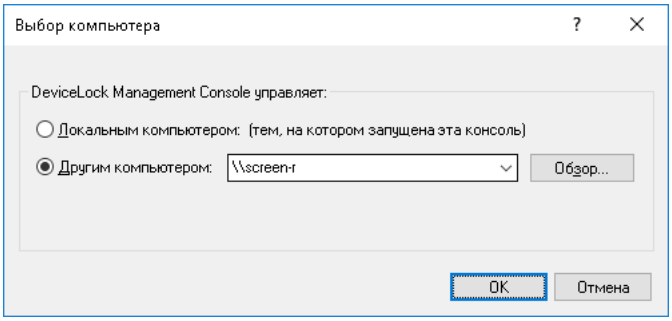
Чтобы подключиться к компьютеру, на котором работает сервис DeviceLock, сервер DeviceLock Enterprise Server или сервер DeviceLock Content Security Server, используйте команду **Подключиться** из контекстного меню или соответствующую кнопку на панели инструментов.





Можно подключиться одновременно к сервису DeviceLock, серверу DeviceLock Enterprise Server и серверу DeviceLock Content Security Server, даже если они работают на разных компьютерах.

В диалоговом окне, которое появляется при выборе команды **Подключиться**, выберите параметр **Локальным компьютером** для подключения к компьютеру, на котором в данный момент работает консоль. Чтобы подключиться к другому компьютеру, выберите параметр **Другим компьютером** и укажите имя или IP-адрес компьютера. Перед именем компьютера добавьте 2 обратных слэша: `\\имя_компьютера`. Нажмите кнопку **Обзор**, чтобы выбрать компьютер из списка.



Чтобы подключиться к компьютеру, на котором сервис DeviceLock, сервер DeviceLock Enterprise Server или сервер DeviceLock Content Security Server настроен на использование фиксированного порта, добавьте номер порта в квадратных скобках после имени компьютера, например `\\имя_компьютера[номер_порта]`.

Нажмите **OK**, чтобы подключиться к выбранному компьютеру.

Примечание: Удаленный компьютер должен быть доступен с компьютера, на котором работает консоль управления, иметь совместимую с DeviceLock операционную систему, а также правильно настроенный сетевой протокол TCP/IP. При использовании файрвола, в т.ч. файрвола Windows, его правила должны разрешать соединение с сервисом DeviceLock, сервером DeviceLock Enterprise Server и/или сервером DeviceLock Content Security Server (см. статью DeviceLock по адресу www.devicelock.com/ru/support/kb_view.html?ID=15864).

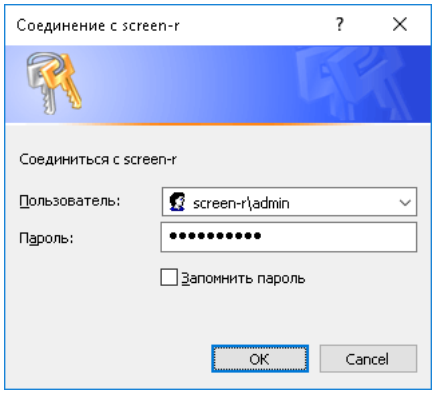
При установке сервис DeviceLock, а также серверы DeviceLock Enterprise Server и DeviceLock Content Security Server автоматически добавляются в список исключений файрвола Windows.

При попытке подключения к компьютеру, на котором сервис DeviceLock не установлен или установлена его устаревшая версия, консоль управления предлагает установить новую версию сервиса DeviceLock. Подробнее об этом см. в разделе Установка в DeviceLock Management Console данного руководства.

При подключении к сервису DeviceLock, который находится в режиме групповых политик, появляется следующее сообщение: "Данная машина сконфигурирована для использования настроек групповых политик. Вы можете переключить ее в режим использования локальной политики. В таком случае настройки групповых политик будут замещены настройками локальной политики." В режиме групповых политик сервис DeviceLock получает настройки из объекта групповой политики, поэтому их изменения, сделанные с помощью консоли DeviceLock Management Console, будут отменены при очередном автоматическом применении групповой политики. См. также описание параметра Использовать групповые/серверные политики в разделе Настройки сервиса данного руководства.

При попытке подключиться к компьютеру, на котором сервер DeviceLock Enterprise Server или DeviceLock Content Security Server не установлен или не запущен, появляется следующее сообщение об ошибке: "В системе отображения конечных точек не осталось доступных конечных точек." DeviceLock Enterprise Server и DeviceLock Content Security Server должны быть установлены и запущены до того, как консоль управления может быть подключена к ним. Инструкции по установке этих серверов см. в разделах Установка DeviceLock Enterprise Server и Установка DeviceLock Content Security Server данного руководства.

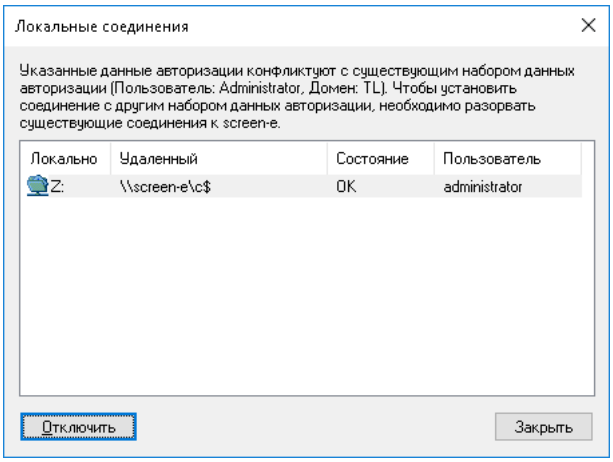
При подключении консоли к компьютеру проверяется, есть ли у текущего пользователя права администратора на этом компьютере. Если текущий пользователь не имеет достаточных прав, появится диалоговое окно для ввода имени и пароля другого пользователя.



В появившемся диалоговом окне укажите имя и пароль пользователя, у которого есть права администратора. Этот пользователь должен быть в списке администраторов DeviceLock, если контроль доступа по умолчанию отключен для сервиса DeviceLock, сервера DeviceLock Enterprise Server или сервера DeviceLock Content Security Server.

При подключении к удаленному компьютеру возможен так называемый "конфликт учетных записей", если локальный компьютер уже подключен к какому-либо ресурсу на удаленном компьютере (например, подключен сетевой диск, открыт общий сетевой ресурс и т.п.) и для подключения консоли к этому компьютеру используются имя и пароль другого пользователя. Windows не допускает несколько подключений к одному компьютеру с использованием разных учетных записей и возвращает следующее сообщение об ошибке: "Указанные данные авторизации конфликтуют с существующим набором данных авторизации." Для разрешения конфликта необходимо разорвать существующие соединения с удаленным компьютером.

Если имеет место “конфликт учетных записей”, консоль DeviceLock Management Console отображает диалоговое окно со списком соединений локального компьютера, предлагая разорвать мешающие соединения.



Выберите в списке все соединения с удаленным компьютером, к которому необходимо подключить консоль, и нажмите кнопку **Отключить**. Затем нажмите кнопку **Закрыть** и попробуйте подключиться к этому компьютеру еще раз.

Примечание: Иногда разорвать существующее соединение не удается, что препятствует подключению консоли к удаленному компьютеру под учетной записью другого пользователя. В этом случае используйте команду **Запуск от имени другого пользователя**, чтобы запустить консоль DeviceLock Management Console под учетной записью администратора сервиса DeviceLock, сервера DeviceLock Enterprise Server и/или сервера DeviceLock Content Security Server. Эта команда появляется в контекстном меню, если щелкнуть правой кнопкой мыши, удерживая клавишу Shift.

Возможные ошибки подключения

При подключении консоли управления к компьютеру могут возникнуть следующие ошибки:

- **(1722) RPC сервер недоступен** - Вы пытаетесь подключиться к компьютеру, который либо не существует (неправильное имя или IP-адрес), либо недоступен. Убедитесь в том, что имя компьютера введено правильно. Попробуйте выполнить команду ping для этого имени или IP-адреса. Попробуйте подключиться к этому компьютеру, используя стандартные средства администрирования Windows (такие как "Управление компьютером", "Службы" и т.п.). Убедитесь, что компьютер работает под управлением ОС, совместимой с DeviceLock.

  Также возможно, что файрвол блокирует доступ к компьютеру. Нужно настроить файрвол, открыв необходимые порты для DeviceLock. Можно настроить DeviceLock для работы по фиксированному TCP-порту, что упростит задачу по настройке файрвола. По умолчанию сервис DeviceLock, сервер DeviceLock Enterprise Server и сервер DeviceLock Content Security Server используют порты 9132, 9133 и 9134 соответственно. Сервис DeviceLock автоматически добавляет себя в список исключений встроенного файрвола Windows.

- **(1753) В системе отображения конечных точек не осталось доступных конечных точек** - Вы пытаетесь подключиться к компьютеру, где сервис DeviceLock, сервер DeviceLock Enterprise Server или сервер DeviceLock Content Security Server недоступен. Прежде всего убедитесь в том, что сервис DeviceLock, сервер DeviceLock Enterprise Server или сервер DeviceLock Content Security Server установлен и запущен на этом компьютере.

  Существует вероятность того, что данный компьютер был только что запущен и Windows в настоящий момент находится в стадии инициализации. Возможно, еще не успела запуститься служба удаленного вызова процедур (Remote Procedure Call, RPC).

  Возможно, что файрвол блокирует доступ к сервису DeviceLock, серверу DeviceLock Enterprise Server или серверу DeviceLock Content Security Server (см. данное выше описание ошибки 1722). О настройке файрвола для поддержки удаленного вызова процедур см. в статье Microsoft по адресу docs.microsoft.com/windows/security/threat-protection/windows-firewall/create-inbound-rules-to-support-rpc.

  Подробнее об ошибках удаленного вызова процедур и способах их устранения см. в статье Microsoft по адресу docs.microsoft.com/windows/client-management/troubleshoot-tcpip-rpc-errors.

- **(5) Доступ запрещен** - У вас недостаточно прав для подключения к удаленному компьютеру. Убедитесь, что консоль управления пытается подключиться к удаленному компьютеру под учетной записью пользователя с правами локального администратора этого компьютера.

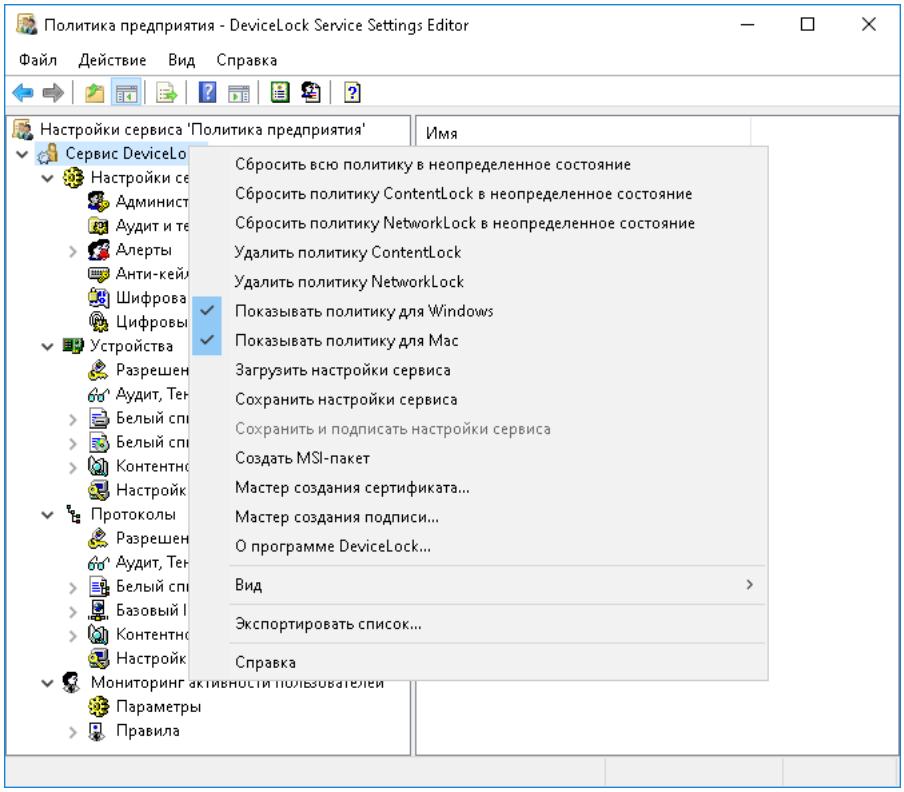
  Возможно, потребуется запустить консоль управления под учетной записью другого пользователя, который обладает необходимыми правами на удаленном компьютере.

- **(7045) Для выполнения данной операции необходимы привилегии администратора** - У вас недостаточно прав для подключения к сервису DeviceLock, серверу DeviceLock Enterprise Server или серверу DeviceLock Content Security Server. Консоль управления пытается подключиться к удаленному компьютеру от имени пользователя, который не входит в список администраторов DeviceLock.

DeviceLock Service Settings Editor

DeviceLock Service Settings Editor используется для создания и редактирования файлов, описывающих настройки, разрешения, правила аудита, теневого копирования и тревожных оповещений.

Консоль DeviceLock Service Settings Editor устанавливается вместе с остальными консолями управления DeviceLock.



Разница между процедурой задания политик в консоли DeviceLock Management Console и DeviceLock Service Settings Editor незначительна, поэтому рекомендуем вначале ознакомится с разделом Управление сервисом DeviceLock для Windows данного руководства.

По сравнению с консолью DeviceLock Management Console использование консоли DeviceLock Service Settings Editor имеет следующие особенности:

- Не требуется подключаться к клиентским компьютерам, т.к. DeviceLock Service Settings Editor работает с файлом настроек сервиса DeviceLock, а не с клиентским компьютером. Все настройки редактируются и сохраняются в файле. Это похоже на работу DeviceLock Group Policy Manager, с тем отличием, что настройки сервиса сохраняются не в объектах групповой политики, а в текстовых файлах настроек.
- Можно установить любой параметр (или все параметры сразу) в состояние **Не задано**. Все такие параметры игнорируются, когда политика применяется к сервису DeviceLock.
- Можно удалить политику ContentLock и/или политику NetworkLock из файла настроек. Применение такого файла настроек к сервису DeviceLock приводит к сбросу всех параметров ContentLock и/или NetworkLock для этого сервиса. Обзор ContentLock и NetworkLock см. в разделе Модули ContentLock и NetworkLock ранее в этом документе.
- Можно удалить любые политики, заданные для автономного режима (разрешения, аудит, правила теневого копирования и оповещений, белые списки и т.д.), как для типов устройств, так и для сетевых протоколов, чтобы принудительно использовать в файле настроек только политики для оперативного режима.

Создание или редактирование политики

Чтобы создать новую политику “с нуля”, откройте консоль DeviceLock Service Settings Editor и вносите необходимые изменения в его чистую политику по умолчанию.

При желании отредактировать существующую политику загрузите файл настроек с этой политикой в редактор используя команду **Загрузить настройки сервиса** из контекстного меню и вносите в нее необходимые изменения.

Примечание: Имя загруженного файла настроек отображается в заголовке окна консоли (например, `Service Settings - [дата время] - DeviceLock Service Settings Editor`).

При создании новой политики “с нуля” используйте команду **Сохранить настройки сервиса** из контекстного меню для сохранения политики в файле. Также можно использовать команду **Сохранить и подписать настройки сервиса** для сохранения политики в файле и автоматического подписывания этого файла с использованием последнего использованного сертификата DeviceLock (секретного ключа). Команда **Сохранить и подписать настройки сервиса** недоступна, если в программе Мастер создания подписи никогда не использовался секретный ключ. Предусмотрена возможность отказа от сохранения SID (идентификаторов безопасности) в файле настроек (см. Варианты сохранения файла настроек).

Файлы настроек, созданные в консоли DeviceLock Service Settings Editor, могут быть загружены с помощью DeviceLock Management Console или DeviceLock Group Policy Manager.

Файлы настроек могут быть отправлены пользователям, чьи компьютеры не подключены к сети, так что файл настроек невозможно загрузить при помощи консолей управления. Чтобы предотвратить внесение несанкционированных изменений, в такой ситуации следует подписывать файлы настроек, используя программу **Мастер создания подписи** и сертификат DeviceLock (секретный ключ). О том, как подписать файл настроек, см. Настройки сервиса в разделе Мастер создания подписи данного руководства.

Если выполняется редактирование существующей политики, DeviceLock Service Settings Editor автоматически сохранит внесенные изменения.

Примечание: Только явно заданные параметры из файла настроек применяются к клиентским компьютерам. Все параметры в состоянии **Не задано** игнорируются клиентскими компьютерами.

DeviceLock Service Settings Editor также используется в подключаемом модуле **Установить настройки сервиса** для DeviceLock Enterprise Manager. Этот подключаемый модуль запускает DeviceLock Service Settings Editor как внешнее приложение и открывает в нем файл настроек, выбранный для данного модуля.

При внесении изменений в файл настроек, открытый на редактирование модулем **Установить настройки сервиса**, все изменения сохраняются в этом файле автоматически. По завершении редактирования просто закройте DeviceLock Service Settings Editor и вернитесь в диалог настройки модуля.

Для получения дополнительной информации см. описание модуля Установить настройки сервиса в разделе DeviceLock Enterprise Manager данного руководства.

Варианты сохранения файла настроек

При сохранении файла настроек можно выбрать один из следующих вариантов:

- **Файлы настроек DeviceLock** - Сохраненный файл будет содержать самую полную информацию о пользователях, которым назначены политики и правила DeviceLock в этом файле, включая имена пользователей, групп, доменов и компьютеров, а также SID (идентификаторы безопасности).
- **Файлы настроек DeviceLock - Имена пользователей в формате FQDN** - Сохраненный файл не будет содержать идентификаторы безопасности, кроме идентификаторов хорошо известных локальных пользователей и групп (СИСТЕМА, Администраторы и т.п.). Имена учетных записей будут указаны в формате `<имя домена>\<имя пользователя>`.
- **Файлы настроек DeviceLock - Имена пользователей** - Сохраненный файл не будет содержать идентификаторы безопасности, кроме идентификаторов хорошо известных локальных пользователей и групп. Имена учетных записей будут указаны в формате `<имя пользователя>` без указания имени домена или компьютера.

Сохранение файла настроек без идентификаторов безопасности и имен доменов/компьютеров может потребоваться, когда необходимо применить файл к автономным компьютерам, на каждом из которых имеется один и тот же набор имен локальных пользователей. В этом случае файл должен идентифицировать пользователей по имени без указания идентификаторов безопасности или имен доменов/компьютеров; в противном случае сервис DeviceLock не сможет обнаружить имена пользователей на компьютере, отличном от того, на котором данный файл настроек был сохранен.

DeviceLock Group Policy Manager

Помимо стандартных возможностей управления, предоставляемых в консоли Консоли и инструменты DeviceLock, имеется и более мощный механизм: для настройки и применения разрешений, правил аудита и других параметры сервиса DeviceLock можно использовать групповую политику службы каталогов Active Directory, что позволяет централизованно управлять конфигурацией сервиса DeviceLock на компьютерах, подключенных к домену Active Directory.

Поддержка групповой политики позволяет администрировать сервис DeviceLock, настраивая и применяя параметры политики в консоли "Управление групповой политикой" (Group Policy Management Console, GPMC).

Тесная интеграция в Active Directory является очень важной функцией DeviceLock, поскольку упрощает управление и развертывание DeviceLock Service в больших сетях, без установки дополнительного сервера. DeviceLock не требует собственных серверных компонентов для управления компьютерами в сети, вместо этого используются стандартные функции службы Active Directory.

Посредством групповой политики можно:

- Установить сервис DeviceLock на всех компьютерах локальной сети, даже на те, которые в данный момент не работают или только подключаются к сети. Подробнее см. в разделе Установка через групповые политики данного руководства.
- Контролировать и настраивать сервис DeviceLock на большом количестве компьютеров в различных доменах/подразделениях одновременно. Даже если какие-то компьютеры выключены или отсутствуют в сети, настройки сервиса DeviceLock будут автоматически установлены на таких компьютерах после их подключения к сети.
- Просматривать применяемую и результирующую политики. Подробнее см. в разделе Использование Resultant Set of Policy (RSoP) данного руководства.

Примечание: Для управления DeviceLock при помощи групповых политик необходимо установить и настроить Active Directory. Инструкции по установке и настройке Active Directory см. в документации Microsoft.

О применении групповых политик

Политики обновляются при запуске компьютера. Когда пользователь включает компьютер, система применяет политику для DeviceLock.

Опционально политики могут обновляться на периодической основе. По умолчанию политика обновляется каждые 90 минут. Чтобы задать другой интервал, через который политика будет обновляться, используйте **Редактор объектов групповой политики**. Более подробно об этом читайте в базе знаний Microsoft по адресу support.microsoft.com/kb/203607.

Политики также могут быть обновлены по требованию. Для немедленного обновления текущих политик, администратор может вызвать утилиту командной строки: `gpupdate.exe /force`, предоставляемую операционной системой Windows.

При применении политики система запрашивает у службы каталогов список объектов групповой политики (GPO), которые нужно обработать. При обновлении политики система запрашивает у Active Directory список объектов групповой политики. Каждый объект групповой политики связан с контейнером служб каталогов, содержащему компьютеры. Компьютер получает установки последнего обработанного контейнера службы каталогов Active Directory.

Обрабатывая объекты групповой политики, система проверяет список управления доступом (ACL), связанный с каждым объектом. Если запись управления доступом (ACE) запрещает доступ компьютера к объекту групповой политики, система не применит политики, определенные в этом объекте. Если запись управления доступом дает доступ к объекту, система применяет политики этого объекта.

Стандартные правила наследования политик

Любые неопределенные (не заданные) настройки в объекте политики (GPO) игнорируются, поскольку они не наследуются вниз по дереву. Только определенные (заданные) настройки наследуются.

Возможны три сценария:

- У родителя есть поле для настройки, а у потомка - нет.
- У родителя есть поле для настройки, а у потомка - не конфликтующее с ним поле для этой же настройки.
- У родителя есть поле для настройки, а у потомка - конфликтующее с ним поле для этой же настройки.

Если у GPO есть настройки, заданные для родительской организационной единицы, а у потомка для дочерней организационной единицы эти политики не настроены, потомок наследует родительские настройки GPO.

Если объект политики содержит настройки, определенные (заданные) для родительской записи, и они не конфликтуют с настройками, определенными (заданными) для записи потомка, то потомок наследует эти настройки от родителя и также применяет свои собственные настройки.

Если объект политики содержит настройки, определенные (заданные) для родительской записи, которые конфликтуют с настройками, определенными (заданными) для записи потомка, то потомок не наследует эти настройки от родителя, а применяет свои собственные настройки. Т.е. в этом случае настройки потомка имеют приоритет над настройками родителя.

Рекомендации

При включенном параметре Windows BitLocker To Go (см. Шифрование) сервис DeviceLock может препятствовать применению административных шаблонов из объектов групповой политики. Это вызвано тем, что данный параметр запрещает включать настройку групповой политики “Запретить запись на съемные диски, не защищенные BitLocker” (находится в папке `Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Шифрование диска BitLocker\Съемные носители с данными`), в результате чего любая групповая политика с конфликтующим значением этой настройки не будет применена на компьютере.

Для устранения данной проблемы необходимо отключить параметр Windows BitLocker To Go (включен по умолчанию). Если настройки сервиса DeviceLock поступают из объекта групповой политики или из объекта политики сервера (см. Политики DeviceLock Enterprise Server), то параметр Windows BitLocker To Go необходимо явно отключить в этом объекте. В противном случае этот параметр получит значение по умолчанию, т.е. будет включен. При использовании локальных настроек сервиса DeviceLock достаточно отключить этот параметр в консоли DeviceLock Management Console.

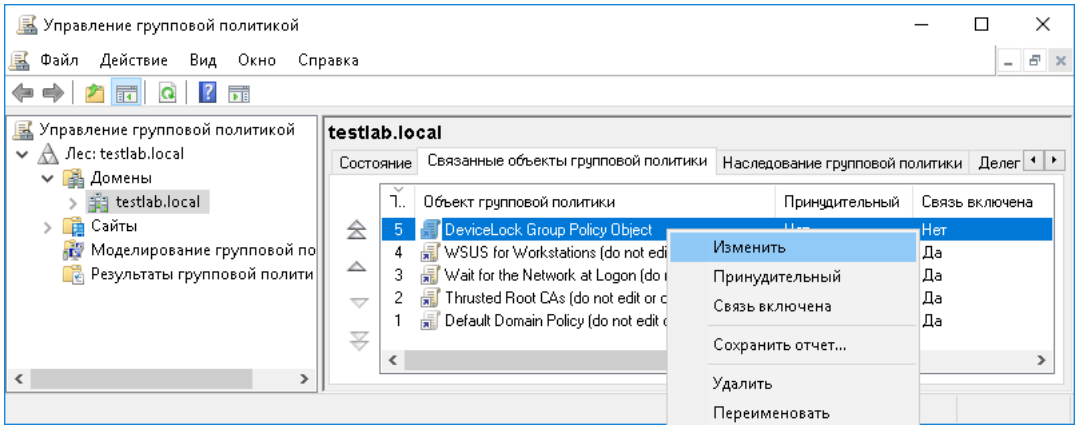
Начало работы с DeviceLock Group Policy Manager

DeviceLock Group Policy Manager интегрируется в редактор объектов групповой политики Windows и не доступен как отдельное приложение. Чтобы использовать DeviceLock Group Policy Manager на вашем локальном компьютере, а не на контроллере домена, на ваш компьютер необходимо установить консоль “Управление групповой политикой” (Group Policy Management console, GPMC).

Для Windows Server 2003 или Windows XP консоль “Управление групповой политикой” можно скачать с сайта Microsoft microsoft.com/download/details.aspx?id=21895. Для более поздних версий клиентской операционной системы Windows необходимо установить средства удаленного администрирования сервера (Remote Server Administration Tools, RSAT). Инструкции по их установке можно найти в статье Microsoft support.microsoft.com/kb/2693643.

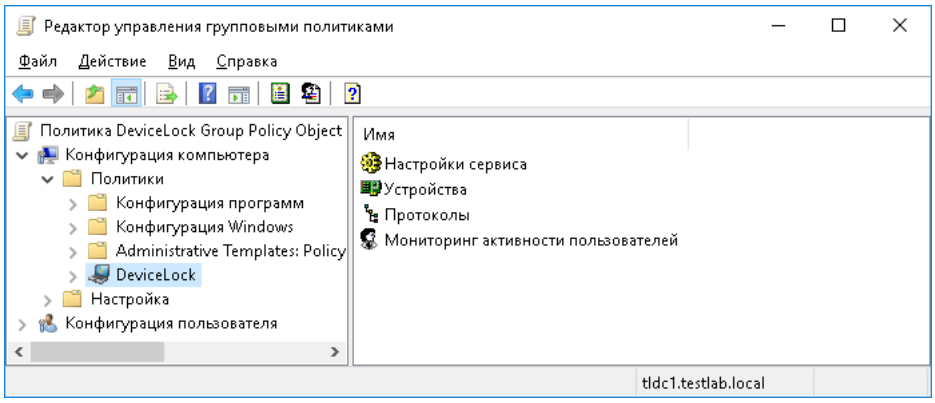
Для доступа к DeviceLock Group Policy Manager выполните следующие действия:

1. Запустите консоль “Управление групповой политикой”.
2. В дереве консоли выберите необходимый домен Active Directory.
3. На вкладке **Связанные объекты групповой политики** на панели сведений щелкните правой кнопкой мыши нужный объект групповой политики и выберите команду **Изменить**.



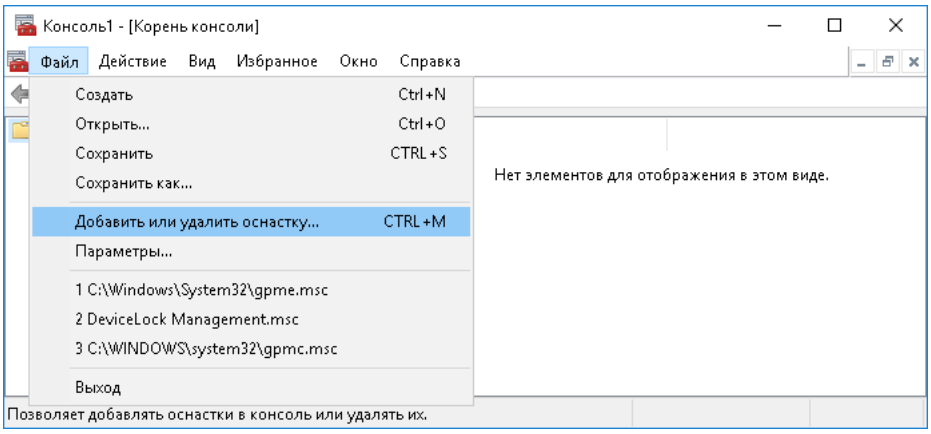
   Если требуется создать новый объект групповой политики, щелкните правой кнопкой мыши домен в дереве консоли и выберите команду **Создать объект групповой политики в этом домене и связать его**.

4. Подождите, пока запустится редактор управления групповыми политиками. Это может занять какое-то время.
5. В разделе **Конфигурация компьютера** выберите пункт **DeviceLock**.

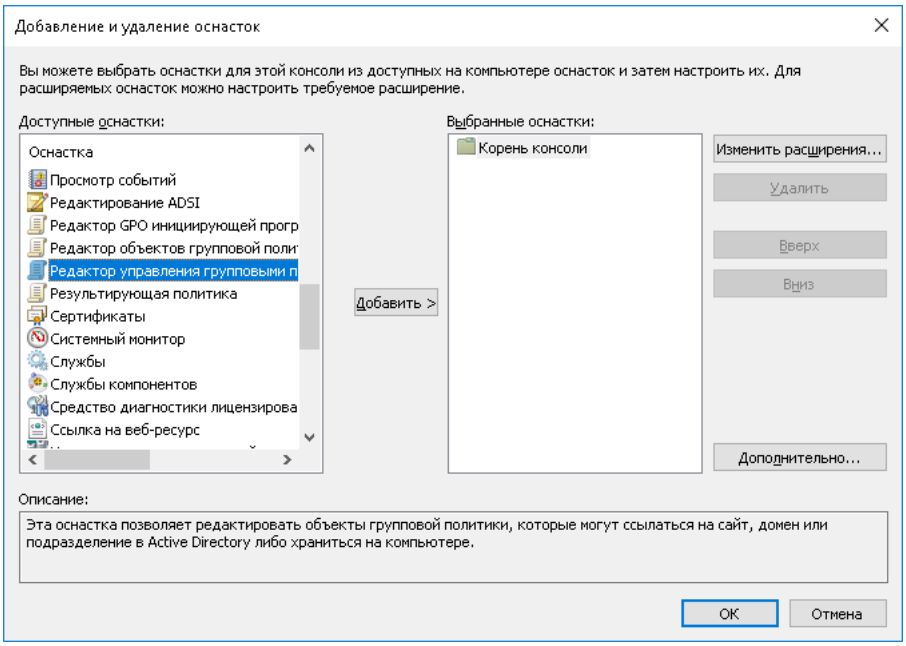


Можно также запустить консоль управления MMC и вручную добавить оснастку **Редактор управления групповыми политиками**:

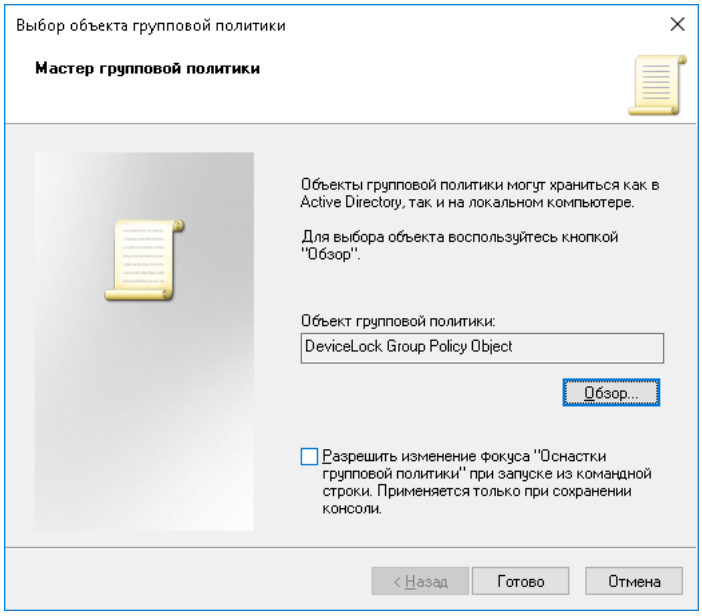
1. Запустите **mmc** из командной строки или используйте для этого команду **Выполнить**.
2. Откройте меню **Файл** и выберите команду **Добавить или удалить оснастку**.



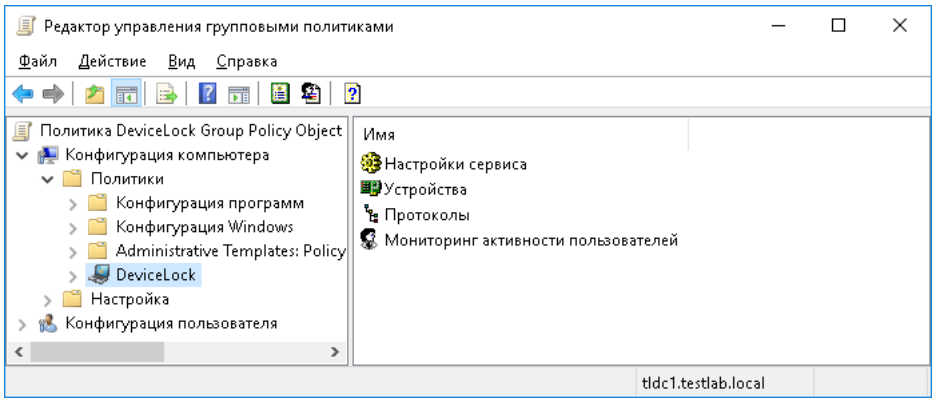
3. В появившемся диалоговом окне выберите оснастку **Редактор управления групповыми политиками** и нажмите кнопку **Добавить**.



4. Нажмите кнопку **Обзор**, чтобы выбрать нужный объект групповой политики из домена Active Directory, затем нажмите кнопку **Готово**.



5. Нажмите **OK**, чтобы закрыть диалоговое окно **Добавление и удаление оснасток**.
6. В разделе **Конфигурация компьютера** выберите пункт **DeviceLock**.



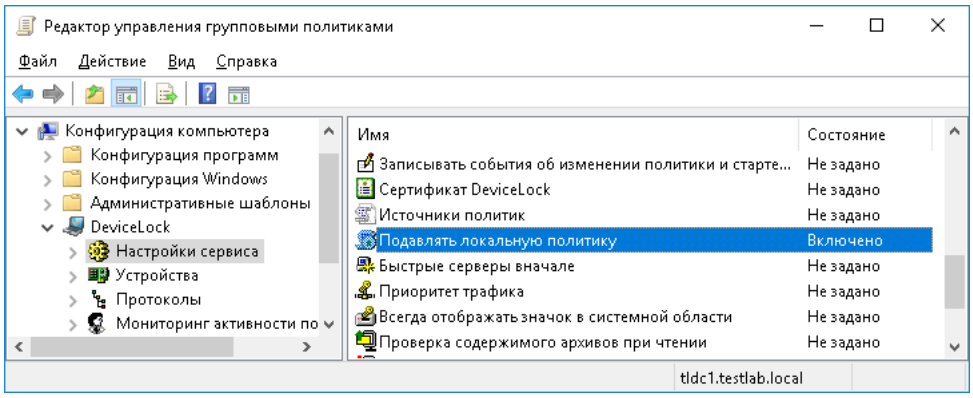
Использование DeviceLock Group Policy Manager

Разница между администрированием через консоль DeviceLock Management Console и DeviceLock Group Policy Manager незначительна. Для получения дополнительной информации см. раздел Управление сервисом DeviceLock для Windows.

Используя DeviceLock Group Policy Manager, невозможно управлять сервером DeviceLock Enterprise Server и просматривать журналы. Для этого следует использовать консоль Консоли и инструменты DeviceLock.

По сравнению с консолью DeviceLock Management Console, DeviceLock Group Policy Manager предоставляет четыре дополнительных функции:

1. Параметр **Подавлять локальную политику**. При необходимости запретить изменение настроек в обход групповых политик (Group Policy) или серверных политик (см. раздел Политики DeviceLock Enterprise Server), установите значение **Включено** для параметра **Подавлять локальную политику** в узле **Настройки сервиса**. Это принудительно включит режим групповой или серверной политики для всех компьютеров, входящих в соответствующий объект политики.



Если параметр **Подавлять локальную политику** включен, параметр **Использовать групповые/серверные политики** в настройках сервиса DeviceLock не может быть выключен в консоли DeviceLock Management Console или DeviceLock Enterprise Manager.

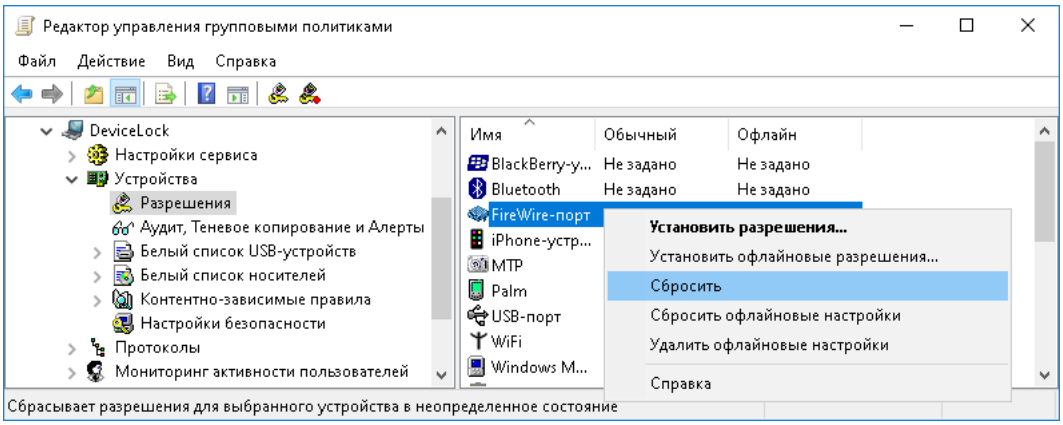
Следующая таблица показывает, как параметры **Использовать групповые/серверные политики** и **Подавлять локальную политику** влияют на режим применения политики.

Использовать групповые/серверные политики	Подавлять локальную политику	Режим применения политики
Отключено	Отключено	Применяется только локальная политика.
Включено	Включено	Применяется только групповая или серверная политика.
Включено	Отключено	Применяется групповая или серверная политика. Локальная политика может действовать до очередного автоматического применения групповой или серверной политики.

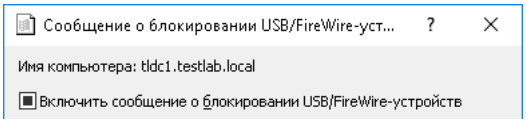
При настройке параметра **Подавлять локальную политику** необходимо учесть следующее:

- Когда параметр **Подавлять локальную политику** выключен, а параметр **Использовать групповые/серверные политики** включен, настройки сервиса DeviceLock можно изменить при помощи консоли DeviceLock Management Console или DeviceLock Enterprise Manager. Однако эти изменения будут отменены при очередном автоматическом применении групповых или серверных политик.
- При выключенном параметре **Подавлять локальную политику** все изменения в настройках сервиса DeviceLock, внесенные при помощи консоли DeviceLock Management Console или DeviceLock Enterprise Manager, вступают в силу немедленно.

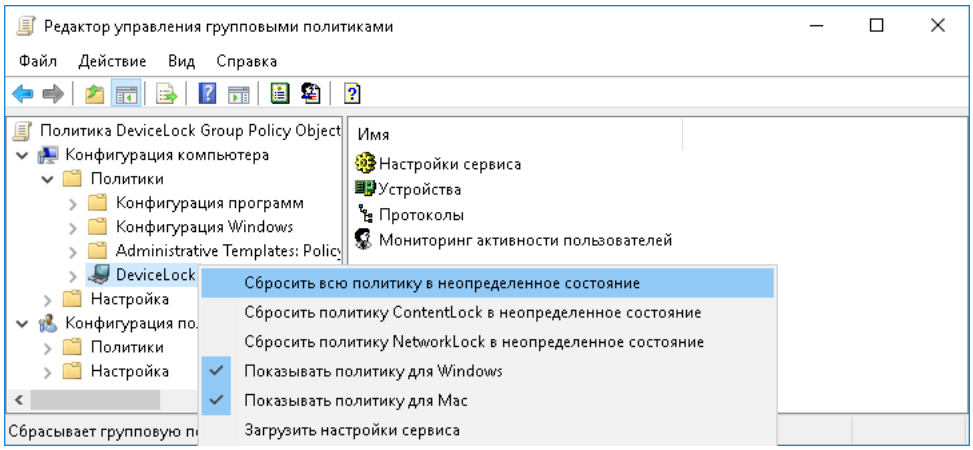
2. Состояние **Не задано** для параметров. Любой параметр можно перевести в состояние **Не задано**. Все параметры, которые находятся в этом состоянии, игнорируются в объекте групповой политики. Для получения дополнительной информации см. раздел Стандартные правила наследования политик данного руководства.



Чтобы перевести параметр в состояние **Не задано**, используйте команду **Сбросить** из контекстного меню, доступного по нажатию правой кнопки мыши на этом параметре. Также в некоторых диалогах можно использовать промежуточное (серое) состояние флажка, чтобы установить соответствующий параметр в состояние **Не задано**.



3. Сброс всех параметров в состояние **Не задано**. Можно установить все параметры в состояние **Не задано** одним кликом мыши. При этом происходит то же самое, что и при последовательном сбросе каждого параметра (см. выше).



Для сброса всех параметров в состояние **Не задано** используйте команду **Сбросить всю политику в неопределенное состояние** из контекстного меню узла **DeviceLock**. Появится сообщение с запросом подтверждения операции: “Сброс политики DeviceLock в неопределенное состояние - необратимое действие. Все настройки DeviceLock будут потеряны. Вы действительно хотите продолжить?”

4. Удаление настроек, заданных для автономного режима. Имеется возможность удалить все ранее заданные политики безопасности для автономного режима (разрешения, аудит, правила теневого копирования и тревожных оповещений, белые списки и т.д.) как для типов устройств, так и для сетевых протоколов, чтобы принудительно использовать только политики оперативного режима в этом объекте групповых политик (GPO). Для этого щелкните правой кнопкой мыши на любом параметре политики и выберите команду **Удалить офлайновые настройки**.

Примечание: Для того чтобы управлять настройками сервиса DeviceLock через групповые политики, сервис DeviceLock должен быть установлен и запущен на всех компьютерах, входящих в объект групповой политики. Дополнительную информацию относительно установки агентов вы можете найти в разделе Развертывание сервиса DeviceLock для Windows данного руководства.

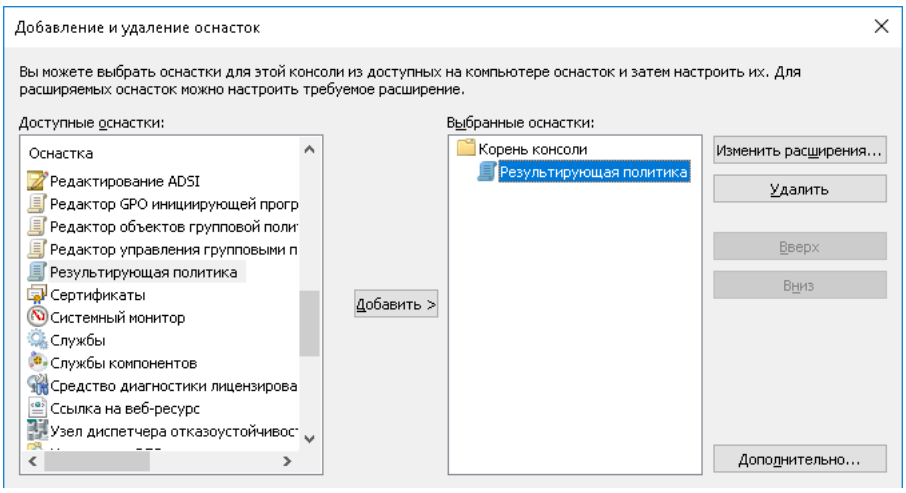
Также не забудьте, что групповая политика обновляется периодически (по умолчанию, каждые 90 минут), следовательно, ваши изменения не вступят в силу немедленно. Для получения дополнительной информации см. раздел О применении групповых политик.

Использование Resultant Set of Policy (RSoP)

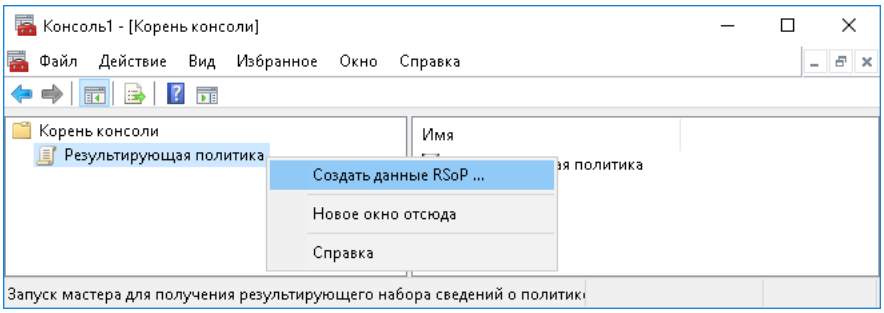
DeviceLock поддерживает Resultant Set of Policy (RSoP). Можно использовать оснастку Windows **Результирующая политика** для просмотра актуально применяемой политики DeviceLock и для проверки результирующей политики, которая будет применена в заданной ситуации.

Чтобы использовать RSoP, запустите консоль MMC и добавьте оснастку **Результирующая политика** следующим образом:

1. Запустите **mmc** из командной строки или используйте для этого команду **Выполнить**.
2. Откройте меню **Файл** и выберите команду **Добавить или удалить оснастку**.
3. В появившемся диалоговом окне выберите из списка оснастку **Результирующая политика** и нажмите кнопку **Добавить**.



4. Нажмите **OK**, чтобы закрыть диалоговое окно **Добавление и удаление оснасток**.
5. В дереве консоли щелкните правой кнопкой мыши элемент **Результирующая политика** и выберите команду **Создать данные RSoP** в контекстном меню.



6. Пройдите через все страницы появившегося мастера, чтобы собрать необходимые данные и построить результирующую политику.
7. В дереве консоли разверните узел **Результирующая политика** и выберите **DeviceLock** в разделе **Конфигурация компьютера**.

Следует помнить, что RSoP не позволяет изменять политики - все настройки доступны только для просмотра.

RSoP очень полезен для понимания того, какой конкретно объект групповой политики применяется или будет применен для выбранного компьютера.

Подробнее о использовании результирующей политики см. в статье Microsoft по адресу technet.microsoft.com/library/cc758010.aspx.

Управления сервисом DeviceLock для Mac через групповые политики

Сервис DeviceLock для Mac может получать настройки из домена Active Directory через сервер DeviceLock Enterprise Server. Чтобы разрешить сервису DeviceLock для Mac принимать настройки из групповых политик, выполните следующие шаги:

1. Зарегистрируйте компьютер Mac в домене Windows.
2. Поместите добавленный компьютер в требуемый OU и настройте политики доступа в соответствии с вашими требованиями.
3. Установите сервер DeviceLock Enterprise Server. Специфических требований по настройке сервера нет. Убедитесь, что компьютер, на котором установлен сервер DeviceLock Enterprise Server, имеет доступ к контроллеру домена, в котором зарегистрирован компьютер Mac.
4. На компьютере Mac укажите адрес сервера DeviceLock Enterprise Server, настроенного на предыдущем шаге.

Групповые политики будут применяться к компьютеру Mac в следующих случаях:

- При перезагрузке операционной системы.
- Ежечасно.
- При изменении параметра DeviceLock Enterprise Server(ы) в узле Настройки сервиса дерева консоли.
- В случае принудительного обновления политик.

Для принудительного обновления политик можно использовать следующую команду:

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

DeviceLock Enterprise Manager

С помощью DeviceLock Enterprise Manager можно просматривать и изменять политики безопасности, заданные для типов устройств и протоколов, осуществлять установку, обновление и удаление агентов, а также просматривать журналы аудита и теневого копирования для всех компьютеров большой сети. Мы рекомендуем использовать DeviceLock Enterprise Manager в сети без Active Directory.

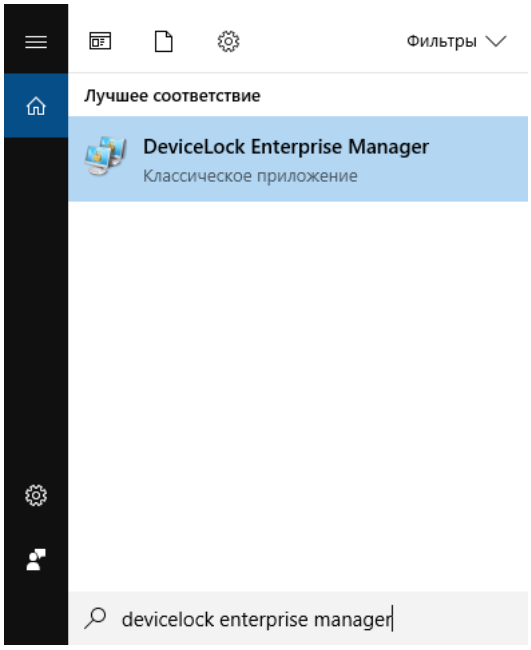
Основанный на многопоточности, DeviceLock Enterprise Manager ускоряет выполнение всех действий для всех компьютеров в большой сети.

DeviceLock Enterprise Manager сохраняет, сравнивает и фильтрует данные, получаемые им со всех компьютеров. Администраторы могут делать “снимки” систем для последующего сравнения и записи изменений.

DeviceLock Enterprise Manager имеет гибкую архитектуру, позволяющую подключать модули (плагины) по мере необходимости. Каждый модуль отрабатывает свою задачу и отображает полученную информацию в своем собственном окне.

Инструкции по установке DeviceLock Enterprise Manager см. в разделе Установка консолей управления данного руководства.

Чтобы открыть DeviceLock Enterprise Manager, найдите и выберите это приложение на стартовой странице Windows:

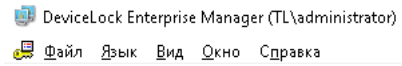


Пользовательский интерфейс

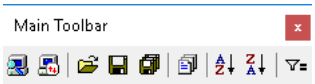
Консоль DeviceLock Enterprise Manager имеет многодокументный интерфейс (MDI), что позволяет использовать отдельное окно для каждой выполняемой задачи.

Размер основного окна можно изменять. DeviceLock Enterprise Manager сохраняет его размер и расположение и восстанавливает их при следующем запуске.

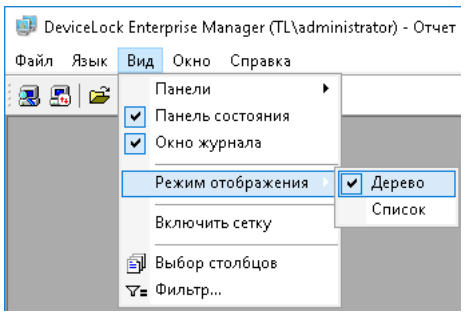
Многие функции программы доступны через главное меню основного окна:



Для изменения списка столбцов, отображаемых в окнах модулей, используйте пункт **Выбор столбцов** в меню **Вид** или соответствующую кнопку на основной панели инструментов (Main Toolbar).

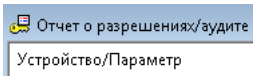


По умолчанию DeviceLock Enterprise Manager отображает информацию из подключаемых модулей в виде дерева. Однако информацию можно просмотреть и в виде неформатированного текста. Для изменения режима отображения выберите пункт **Режим отображения** в меню **Вид** и затем выберите либо опцию **Дерево**, либо **Список**. Этот режим устанавливается для каждого модуля индивидуально.



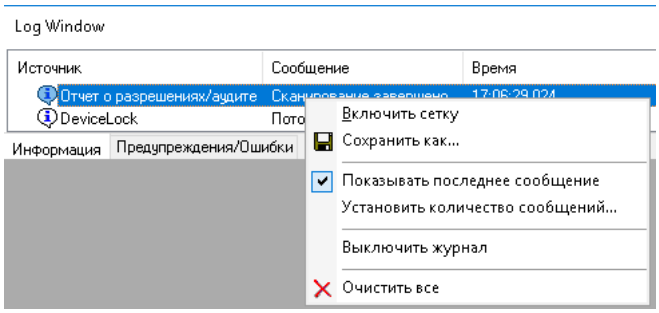
Вы можете скрыть панель статуса и/или окно журнала, выбрав соответствующие подпункты в меню **Вид**. Для того чтобы в окне модулей значения были разделены сеткой, выберите подпункт **Включить сетку** в меню **Вид**. Этот режим устанавливается для каждого модуля индивидуально.

Чтобы отсортировать данные в окне какого-либо модуля, щелкните заголовок столбца. Для обратного порядка сортировки щелкните заголовок еще раз.



Если необходимо отсортировать данные верхнего уровня в дереве (такие, как домены или компьютеры), используйте соответствующую кнопку на основной панели инструментов:

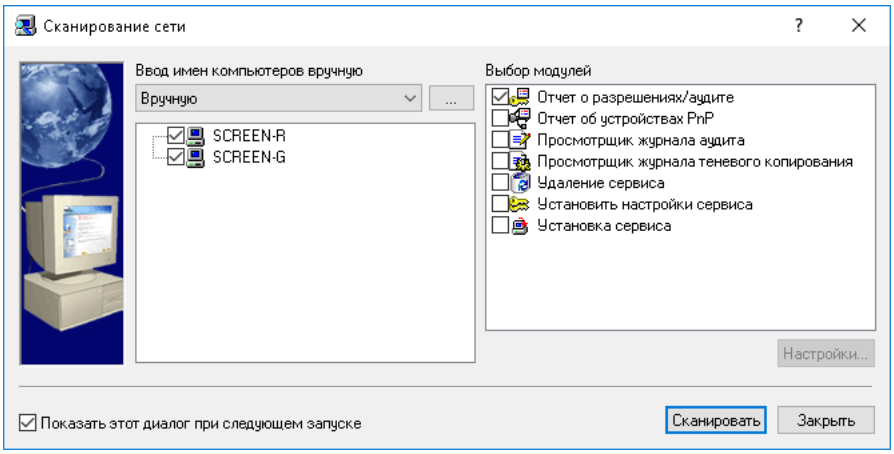
Многие функции программы доступны через главное меню основного окна. Окно журнала отображает полезную информацию о выполняемых операциях, а также диагностические сведения и сообщения об ошибках. Есть два списка журналов: **Информация** и **Предупреждения/Ошибки**.



С помощью правой клавиши мыши в окне журнала вызывается контекстное меню.

Диалоговое окно “Сканирование сети”

Диалоговое окно **Сканирование сети** обеспечивает возможность выбора компьютеров в локальной сети и выполнения действий (установка или удаление агента, установка разрешений, правил аудита и т.п.), которые должны быть выполнены для этих компьютеров.



Чтобы открыть окно **Сканирование сети**, выберите команду **Сканировать сеть** из меню **Файл** или нажмите соответствующую кнопку на панели инструментов. Если установлен флажок **Показать этот диалог при следующем запуске**, окно **Сканирование сети** будет открываться автоматически при каждом запуске консоли DeviceLock Enterprise Manager.

Далее описаны три простых шага, которые позволят управлять сервисом DeviceLock на компьютерах в локальной сети.

Выбор компьютеров

Первый шаг - выбор компьютеров. Можно использовать контекстное меню, доступное по нажатию правой кнопки мыши, чтобы выбирать необходимые элементы (типы компьютеров, домены или компьютеры).

DeviceLock Enterprise Manager предоставляет несколько способов для выбора компьютеров.

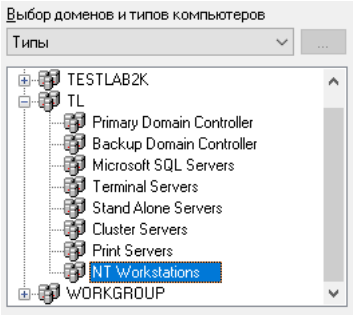
- Сетевые компьютеры могут быть выбраны по их типам.

  Каждый тип представляет все компьютеры, относящиеся к выбранной категории:

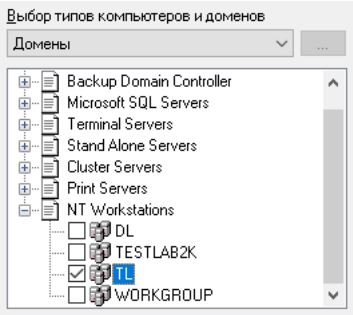
  - Primary Domain Controller - Основной контроллер домена.
  - Backup Domain Controller - Резервный контролер домена.
  - Microsoft SQL Servers - Любой компьютер с запущенным сервером Microsoft SQL.
  - Terminal Servers - Любой сервер, на котором запущены службы терминала.
  - Stand Alone Servers - Любой сервер, не являющийся котроллером домена.
  - Cluster Servers - Кластер серверов, доступный в домене.
  - Print Servers - Любой компьютер, на котором имеется принтер общего доступа.
  - NT Workstations - Любая рабочая станция под управлением Windows XP/Vista/7/8/10 или Windows Server 2003/2008/2012/2016/2019.

  Ниже представлены два способа выбора компьютеров по типам:

  1. **Типы** - Вы выбираете домен и затем тип компьютеров, с которыми вы собираетесь работать в этом домене.



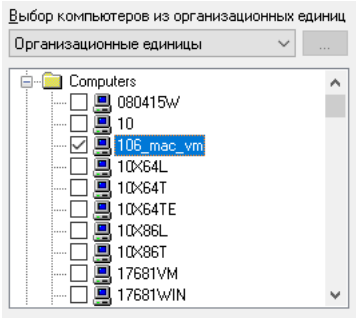
  2. **Домены** - Вы вначале выбираете тип компьютера и затем домен, с компьютерами которого вы собираетесь работать.



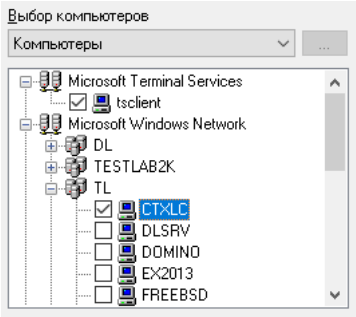
- Сетевые компьютеры также могут быть выбраны по их именам.

  Есть несколько вариантов выбора компьютеров по именам:

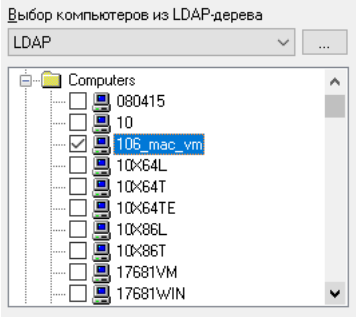
  1. **Организационные единицы** - Вы просматриваете подразделения в Active Directory и выбираете компьютеры, с которыми собираетесь работать.



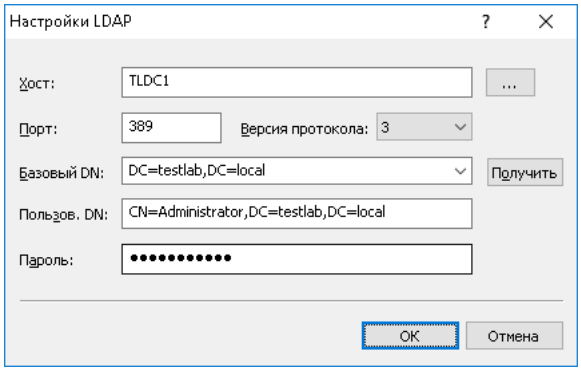
  2. **Компьютеры** - Вы просматриваете дерево сети и выбираете компьютеры.



  3. **LDAP** - Вы выбираете компьютеры из дерева LDAP-совместимой службы каталогов.



  Чтобы настроить подключение к LDAP-серверу, нажмите кнопку ...



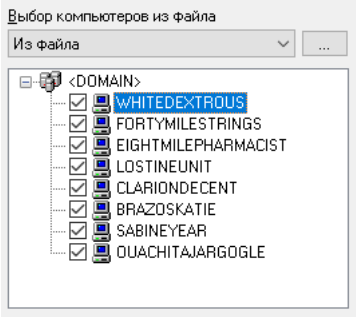
Заполните появившееся диалоговое окно **Настройки LDAP**:

- **Хост** - Имя или IP-адрес LDAP-сервера, к которому выполняется подключение.
- **Порт** - Номер порта, по которому LDAP-сервер принимает подключения. По умолчанию это порт 389.
- **Версия протокола** - Версия LDAP-протокола. Некоторые серверы не полностью поддерживают протокол LDAP v.3, поэтому для выполнения LDAP-запросов на них потребуются изменения в формате взаимодействия. Если выбрана версия **2**, то запросы для сервера будут соответствовать протоколу LDAP v.2.
- **Базовый DN** - Начальная точка для просмотра дерева каталога. Строка DN должна быть в LDAP-формате (например, `cn=users,o=company,c=US`). Оставьте это поле пустым для просмотра с корня дерева.

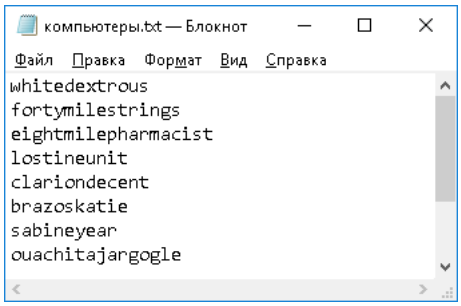
  Нажмите кнопку **Получить**, чтобы получить все доступные контексты службы каталогов для базового DN.
- **Пользов. DN**, **Пароль** - Имя пользователя и пароль для подключения к LDAP-серверу. Строка DN должна быть в LDAP-формате (например, `cn=admin,o=company,c=US`).

4. **Из файла** - Вы загружаете заранее подготовленный список компьютеров из внешнего текстового файла, а затем выбираете компьютеры.

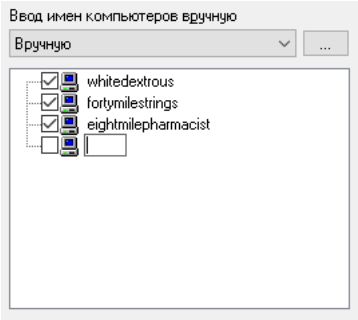
   Чтобы открыть внешний файл, нажмите кнопку ...



Текстовый файл может содержать имена компьютеров и/или IP-адреса, каждый из которых должен быть записан на отдельной строке, и может быть как в Юникод, так и в не Юникод кодировке. Ниже приведен пример такого файла:



5. **Вручную** - Вы вручную вводите имя или IP-адрес каждого компьютера, а затем выбираете нужные компьютеры. Чтобы сохранить введенное значение, нажмите клавишу ENTER или щелкните свободное пространство в списке.

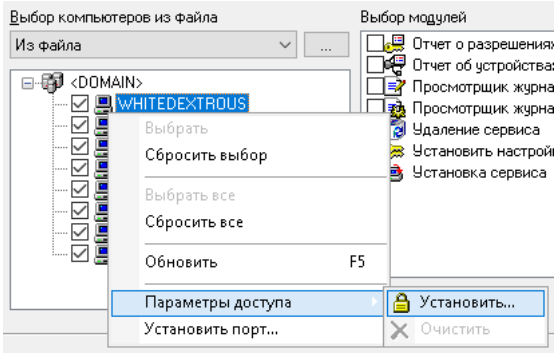


Чтобы добавить запись в список компьютеров, выполните одно из следующих действий:

- Дважды щелкните свободное пространство в списке.
- Щелкните правой кнопкой мыши свободное пространство в списке и нажмите **Добавить** в контекстном меню.
- Щелкните свободное пространство в списке, а затем нажмите клавишу INSERT или клавишу “плюс” (+) на цифровой клавиатуре.
- Нажмите кнопку ..., чтобы для выбора компьютеров использовать диалоговое окно **Выбор: "Компьютеры"**, предоставляемое операционной системой.

Задание альтернативных учетных записей

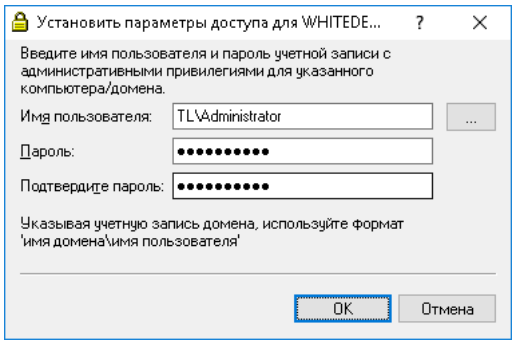
Если для подключения к удаленному компьютеру(-ам) вам требуются данные (пользователь и пароль) альтернативных учетных записей, выберите компьютер или домен из дерева и используйте подменю **Параметры доступа** контекстного меню.



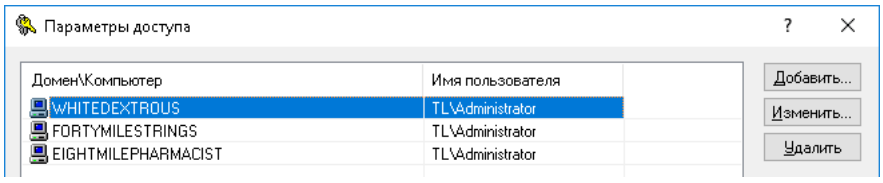
Можно задать альтернативные учетные записи как для отдельного компьютера, так и для всего домена. Чтобы добавить учетные записи, выберите команду **Установить**. Чтобы удалить вспомогательные учетные записи, нажмите **Очистить**.

Данные учетной записи - это имя пользователя и пароль, используемые для аутентификации на удаленных компьютерах. По умолчанию DeviceLock Enterprise Manager использует вашу текущую учетную запись для подключения и работы. Если текущая учетная запись не имеет административных привилегий на удаленных компьютерах, вам потребуется ввести альтернативные учетные записи. DeviceLock Enterprise Manager будет использовать эти записи при подключении к удаленным компьютерам.

Пароли для альтернативных учетных записей всегда сохраняются с использованием шифрования и недоступны никому, за исключением пользователя с правами администратора.



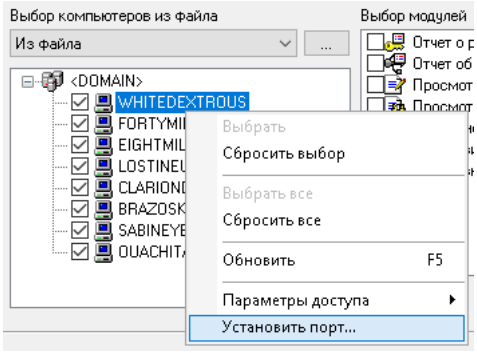
Альтернативные учетные записи также могут быть заданы с использованием диалогового окна **Параметры доступа**. Чтобы открыть окно **Параметры доступа**, выберите пункт **Параметры доступа** из меню **Файл**.



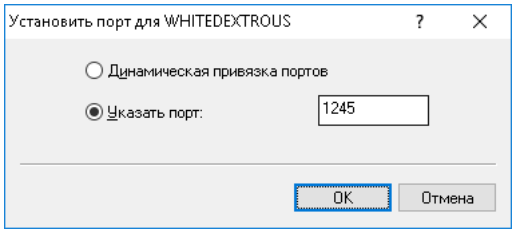
Нажмите кнопку **Добавить**, чтобы задать новые учетные записи. Чтобы изменить существующую запись, выделите ее в списке и нажмите кнопку **Изменить**. Чтобы удалить запись, выделите ее в списке и нажмите кнопку **Удалить**. Для одновременного удаления нескольких записей используйте клавиши Ctrl и/или Shift.

Установка порта

Вы можете установить использование фиксированного TCP-порта для DeviceLock Enterprise Manager. Для этого используйте пункт **Установить порт** из контекстного меню.



DeviceLock Enterprise Manager по умолчанию использует динамическую привязку портов для подключения к сервису DeviceLock. Однако, если на некотором компьютере задан фиксированный порт для сервиса DeviceLock, то для такого компьютера следует выбрать опцию **Указать порт** и ввести номер порта.



Для использования динамических портов выберите опцию **Динамическая привязка портов**.

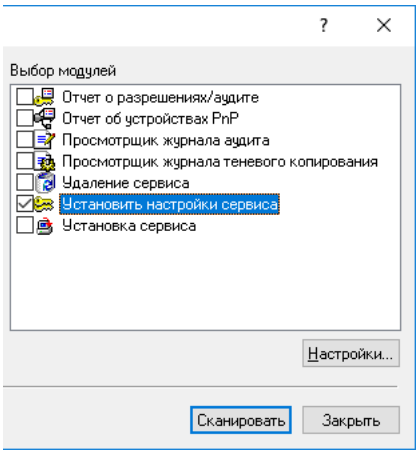
Сервис DeviceLock может быть настроен на использование фиксированного порта или динамических портов в момент установки на компьютер. За дополнительной информацией обращайтесь к разделам Установка без вмешательства пользователя и Установка в DeviceLock Enterprise Manager данного руководства.

Если вам требуется изменить настройку порта, когда сервис DeviceLock уже установлен на компьютере, используйте модуль Установка сервиса.

Информацию о том, какие порты должны быть открыты для того или иного действия, можно получить в разделе Модули данного руководства.

Выбор модуля

Второй шаг - выбор модуля для выполнения задания на компьютерах, которые были выбраны на первом шаге. Для выбора модуля вы можете использовать контекстное меню, доступное по нажатию правой кнопки мыши.



Для задания настроек выбранного модуля используйте кнопку **Настройки**, расположенную под списком модулей. Если модуль не имеет дополнительных настроек, кнопка **Настройки** будет недоступна.

Задания для модуля поступают от DeviceLock Enterprise Manager.

Модуль выполняет задание и возвращает информацию в DeviceLock Enterprise Manager. Полученную от модулей информацию DeviceLock Enterprise Manager отображает в отдельных окнах.

Процесс сканирования

После выбора компьютеров и соответствующего модуля завершающим шагом будет являться процесс сканирования. Нажмите кнопку **Сканировать** для запуска процесса.

Сразу после того, как процесс сканирования запущен, вы можете приступить к просмотру информации, которая возвращается модулем.

Поскольку процесс сканирования запускается в отдельном потоке, вам нет необходимости ожидать окончания сканирования всех компьютеров. Также вы можете в это время выполнять иные действия в интерфейсе DeviceLock Enterprise Manager.

Есть только несколько действий, которые вы не можете выполнять во время сканирования: невозможно закрыть DeviceLock Enterprise Manager и невозможно запустить другой процесс сканирования.

Если по каким-либо причинам вам нужно прервать активный процесс сканирования, выберите пункт **Остановить сканирование** из меню **Файл** или нажмите соответствующую кнопку на панели инструментов.

Процесс сканирования будет прерван, как только модуль вернет управление в DeviceLock Enterprise Manager.

Модули

DeviceLock Enterprise Manager основан на архитектуре, позволяющей подключать модули по мере необходимости. При запуске DeviceLock Enterprise Manager загружает модули из папки `Plugins`, которая расположена в основной папке DeviceLock Enterprise Manager.

DeviceLock Enterprise Manager поставляется со стандартными модулями, которые требуют, чтобы некоторые сетевые порты были открыты, как описано в следующей таблице:

Необходимые порты	Модули
TCP 139 или **TCP 445** **UDP 137** - Этот порт должен быть открыт только когда подключение происходит по имени компьютера. Если используется IP-адрес, то этот порт не нужен.	Просмотрщик журнала аудита Отчет об устройствах PnP
TCP 139 или **TCP 445** **UDP 137** - Этот порт должен быть открыт только когда подключение происходит по имени компьютера. Если используется IP-адрес, то этот порт не нужен.	Установка сервиса Удаление сервиса
TCP 139 или **TCP 445** **TCP 135** - Этот порт должен быть открыт только когда используется подключение по динамическим портам. **TCP** <все порты выше 1024> - Эти порты должны быть открыты только когда используется подключение по динамическим портам. **TCP** <порт> - Этот порт должен быть открыт только когда используется подключение по фиксированному порту. **UDP 137** - Этот порт должен быть открыт только когда подключение происходит по имени компьютера. Если используется IP-адрес, то этот порт не нужен.	Отчет о разрешениях/аудите Установить настройки сервиса Просмотрщик журнала теневого копирования

Подробнее о том, как в DeviceLock Enterprise Manager настроить использование либо динамических портов, либо фиксированного порта, см. в разделе Установка порта.

В момент подключения модуля к удаленному компьютеру возможно возникновение одной из этих ошибок:

- **Версии продукта на машинах клиента и сервера не совпадают (7049)** - Попытка подключиться к компьютеру, на котором установлена и работает старая версия сервиса DeviceLock. Необходимо обновить сервис DeviceLock, используя модуль Установка сервиса.
- **Сетевой путь не найден (53)** - Попытка подключиться к компьютеру, который либо не существует (неправильное имя или IP-адрес), либо недоступен. Убедитесь в том, что имя компьютера введено правильно. Попробуйте подключиться к этому компьютеру, используя стандартные средства администрирования Windows (такие как **Управление компьютером**, **Службы** и т.п.).

  Данная ошибка возникает также когда служба **Server** не запущена на удаленном компьютере. Проверьте службу **Server** и запустите ее, если она остановлена.

Другие ошибки описаны в разделе Возможные ошибки подключения данного руководства.

Из отчета, подготовленного любым модулем, можно открыть консоль DeviceLock Management Console, подключенную к сервису DeviceLock на данном компьютере: щелкните правой кнопкой мыши имя компьютера и выберите команду **Подключиться к сервису DeviceLock**.

Просмотрщик журнала аудита

Модуль **Просмотрщик журнала аудита** получает данные аудита из стандартного журнала Windows.

Чтобы определить максимальный размер журнала аудита и что следует делать в случае его заполнения, используйте команду **Настройки журнала аудита** из контекстного меню доступного по нажатию правой кнопки мыши. Чтобы полностью очистить журнал аудита, используйте команду **Очистить журнал аудита** из контекстного меню.

За дополнительной информацией обращайтесь к разделу Просмотрщик журнала аудита (для компьютера) данного руководства.

Установка сервиса

Модуль **Установка сервиса** устанавливает и/или обновляет сервис DeviceLock на компьютерах.

Примечание: Удаленная установка сервиса DeviceLock на компьютеры под управлением ОС Windows Vista и более поздних версий возможна только с использованием встроенной учетной записи локального администратора. В окружении Windows Active Directory только члены группы "Администраторы домена" могут удаленно устанавливать сервис DeviceLock. Права администратора также требуются для подключения к сервису DeviceLock с помощью консоли DeviceLock Management Console. Дополнительную информацию см. в статье Microsoft по адресу support.microsoft.com/kb/951016.

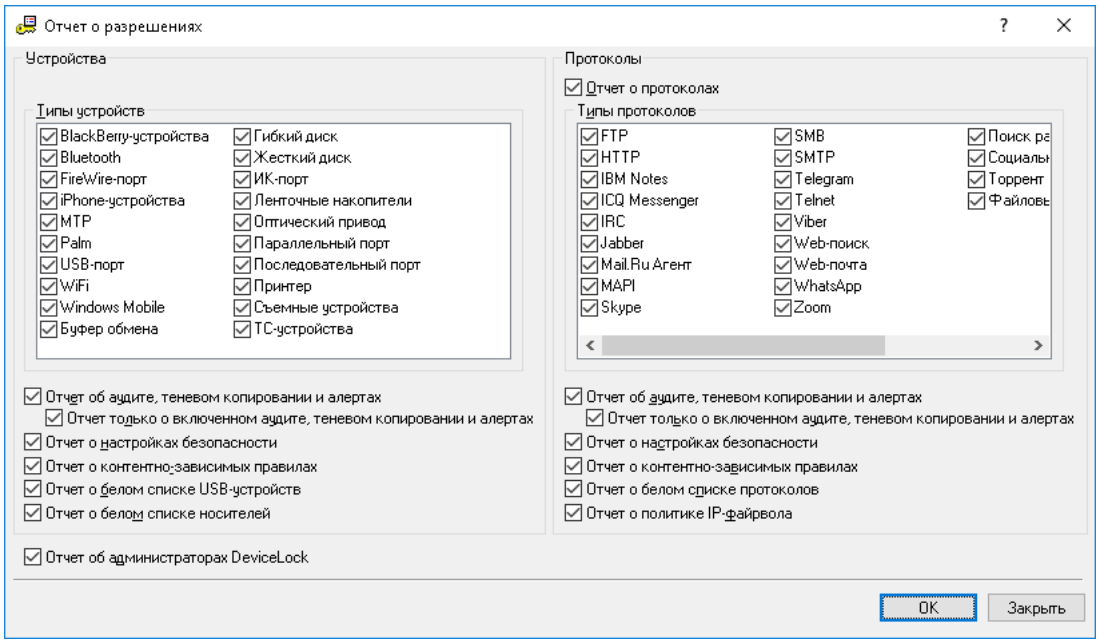
До того, как вы будете использовать этот модуль, необходимо указать местонахождение файлов, необходимых для установки сервиса DeviceLock (файлы `DeviceLock Service.msi`, `DeviceLock Service x64.msi`, `DLRemoteInstaller.exe` и `InstMsiW.exe`). Это можно сделать, нажав кнопку **Настройки**, расположенную под списком модулей в диалоговом окне **Сканирование сети** (см. Выбор модуля).

За дополнительной информацией обращайтесь к разделу Установка в DeviceLock Enterprise Manager.

Отчет о разрешениях/аудите

Модуль **Отчет о разрешениях/аудите** формирует отчет, позволяющий просматривать и изменять политики безопасности, заданные для типов устройств и протоколов.

Перед использованием этого модуля необходимо выбрать информацию, которую для включения в отчет, нажав кнопку **Настройки** под списком модулей в диалоговом окне **Сканирование сети** (см. Выбор модуля).



В появившемся диалоговом окне **Отчет о разрешениях** укажите, какую информацию необходимо включить в отчет.

Чтобы получить информацию о политиках безопасности, заданных для типов устройств, установите соответствующие флажки в области **Устройства**:

- **Отчет об аудите, теневом копировании и алертах** - Включает в отчет информацию об установленных правилах аудита, теневого копирования и оповещений, а также запись о состоянии параметра Записывать события об изменении политики и старте/остановке сервиса.
- **Отчет только о включенном аудите, теневом копировании и алертах** - Исключает из отчета информацию об устройствах, для которых выключен аудит, теневое копирование и оповещения.

  Этот флажок доступен, только если установлен флажок "Отчет об аудите, теневом копировании и алертах".
- **Отчет о настройках безопасности** - Включает в отчет сведения об отключенных дополнительных параметрах безопасности (см. раздел Настройки безопасности (обычный профиль)).
- **Отчет о контентно-зависимых правилах** - Включает в отчет информацию об установленных контентно-зависимых правилах для устройств (см. раздел Правила для устройств главы Контентно-зависимые правила (обычный профиль)).
- **Отчет о белом списке USB-устройств** - Включает в отчет информацию об устройствах, находящихся в белом списке (см. раздел Белый список USB-устройств (обычный профиль)).

- **Отчет о белом списке носителей** - Включает в отчет информацию о носителях, находящихся в белом списке (см. раздел Белый список носителей (обычный профиль)).
- **Отчет об администраторах DeviceLock** - Включает в отчет информацию об учетных записях, которые имеют доступ к сервису DeviceLock.

Чтобы получить информацию о политиках безопасности, заданных для протоколов, установите соответствующие флажки в области **Протоколы**:

- **Отчет о протоколах** - Включает в отчет информацию о политиках безопасности, заданных для протоколов. Если этот флажок не установлен, информация о политиках безопасности, относящихся к контролю сетевых протоколов, будет исключена из отчета.

  Если этот флажок снят, флажки "Отчет об аудите, теневом копировании и алертах" и "Отчет только о включенном аудите, теневом копировании и алертах" будут недоступны.
- **Отчет об аудите, теневом копировании и алертах** - Включает в отчет информацию об установленных для протоколов правилах аудита, теневого копирования и оповещений.
- **Отчет только о включенном аудите, теневом копировании и алертах** - Исключает из отчета информацию о протоколах, для которых выключен аудит, теневое копирование и оповещения.

  Этот флажок доступен, только если установлен флажок "Отчет об аудите, теневом копировании и алертах".
- **Отчет о настройках безопасности** - Включает в отчет информацию о дополнительных параметрах безопасности, заданных для протоколов (см. раздел Настройки безопасности для протоколов).
- **Отчет о контентно-зависимых правилах** - Включает в отчет информацию об установленных контентно-зависимых правилах для протоколов (см. раздел см. раздел Правила для протоколов главы Контентно-зависимые правила (обычный профиль)).
- **Отчет о белом списке протоколов** - Включает в отчет информацию о протоколах, находящихся в белом списке (см. раздел Белый список протоколов).
- **Отчет о политике IP-файрвола** - Включает в отчет информацию о настройках Базового IP-файрвола (см. раздел Базовый IP-файрвол).

В отчет всегда попадает информация об установленном сертификате (см. Сертификаты DeviceLock). Также отчет содержит отдельную запись о том, включен ли параметр Использовать групповые/серверные политики в настройках сервиса DeviceLock.

Отчет об устройствах PnP

Модуль **Отчет об устройствах PnP** формирует отчет, отображающий USB, FireWire и PCMCIA-устройства, которые в текущий момент подключены к компьютерам в локальной сети, и те, что были когда-либо подключены.

Примечание:

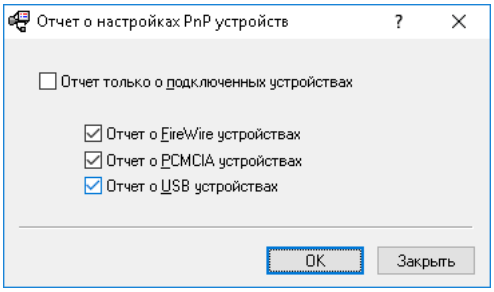
- Для получения списка PnP-устройств с компьютеров, работающих под управлением Windows 8/10 или Windows Server 2012/2016/2019, на этих компьютерах требуется установить сервис DeviceLock.
- Для получения списка PnP-устройств с компьютеров, работающих под управлением Windows Vista / Windows Server 2008 / Windows 7, на этих компьютерах требуется разрешить удаленный доступ к PnP-интерфейсу, изменив в групповую политику (см. статью по адресу www.devicelock.com/ru/support/kb_view.html?ID=15865).

Столбцы отчета описаны ниже:

- **Описание** - Описание устройства, предоставляемое его изготовителем.
- **Информация об устройстве** - Дополнительная информация об устройстве, предоставляемая его изготовителем.
- **Интерфейс подключения** - Интерфейс, через который подключено устройство (USB, FireWire или PCMCIA).
- **Класс** - Класс устройства, определяемый Windows.
- **Описание класса** - Описание класса устройства, определяемого Windows.
- **Подключено** - Флажок, информирующий о том, подключено ли данное устройство в настоящий момент или нет (**Да** или **Нет**).
- **ID-устройства** - Уникальный идентификатор устройства, установленный его изготовителем.
- **Драйвер** - Имя драйвера, который управляет данным устройством.

USB-устройство можно добавить в базу данных DeviceLock, используя контекстное меню, доступное по нажатию правой кнопки мыши (см. раздел База данных USB-устройств).

Перед использованием этого модуля требуется выбрать информацию для включения в отчет. Это можно сделать, нажав кнопку **Настройки**, расположенную под списком модулей в диалоговом окне **Сканирование сети** (см. Выбор модуля).



- **Отчет только о подключенных устройствах** - Установите этот флажок, чтобы включить в отчет информацию об устройствах, подключенных в данный момент к компьютерам. В противном случае вы увидите информацию в том числе и для тех устройств, которые были когда-либо подключены.

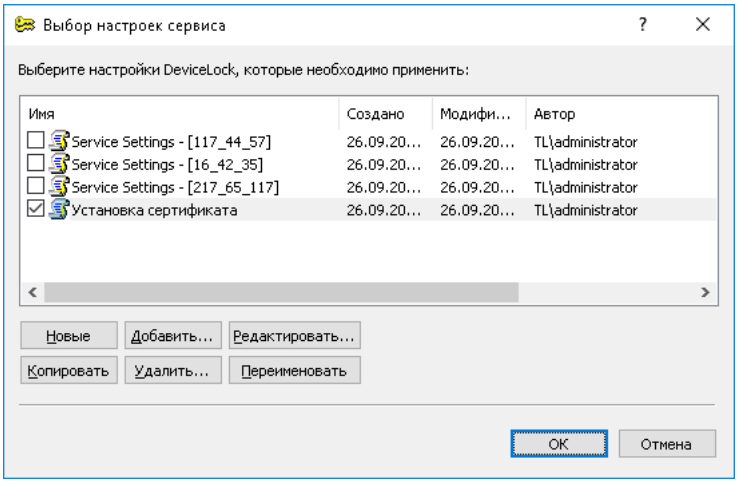
- **Отчет о FireWire устройствах** - Установите этот флажок, чтобы включить в отчет информацию об устройствах, подключенных к FireWire-порту.
- **Отчет о PCMCIA устройствах** - Установите этот флажок, чтобы включить в отчет информацию об устройствах, подключенных через PCMCIA-интерфейс.
- **Отчет о USB устройствах** - Установите этот флажок, чтобы включить в отчет информацию об устройствах, подключенных к USB-порту.

Установить настройки сервиса

Модуль **Установить настройки сервиса** считывает политику (настройки, разрешения, аудит, правила теневого копирования и оповещений) из внешнего файла настроек и устанавливает ее для сервиса DeviceLock на клиентских компьютерах в сети.

Примечание: Только явно заданные параметры из файла политик применяются к клиентским компьютерам. Все параметры в состоянии **Не задано** игнорируются клиентскими компьютерами.

Перед использованием этого модуля вы должны задать настройки, разрешения и/или правила аудита, которые хотите установить. Вы можете сделать это, нажав кнопку **Настройки**, расположенную под списком модулей в окне диалога **Сканирование сети** (см. Выбор модуля).



Прежде всего необходимо подготовить политику для распространения по сети.

Если в списке нет файлов, то можно создать новый файл с чистой политикой, нажав кнопку **Новые**, либо добавить уже существующий файл, нажав кнопку **Добавить**.

Затем выделите файл в списке и нажмите кнопку **Редактировать**, чтобы открыть редактор DeviceLock Service Settings Editor, который используется для создания и редактирования файлов с настройками, разрешениями, аудитом, правилами теневого копирования и оповещений (файлы настроек сервиса DeviceLock). Подробнее см. в разделе DeviceLock Service Settings Editor данного руководства.

Когда вы завершите редактирование политики, отметьте ее файл, поставив флажок рядом с именем в списке. Затем нажмите кнопку **OK**, чтобы закрыть диалог настройки модуля **Установить настройки сервиса**.

Просмотрщик журнала теневого копирования

Модуль **Просмотрщик журнала теневого копирования** получает записи журнала теневого копирования с компьютеров.

Используйте контекстное меню, доступное по нажатию правой кнопки мыши, для доступа к основным функциям модуля.

Для получения дополнительной информации см. раздел Просмотрщик журнала теневого копирования (для компьютера) данного руководства.

Удаление сервиса

Модуль **Удаление сервиса** удаляет сервис DeviceLock, все его настройки и компоненты с компьютеров.

Если учетная запись, под которой этот модуль подключается к компьютеру, не имеет полного административного права на доступ к сервису DeviceLock, то модуль не сможет выполнить операцию удаления.

Похожая ошибка возникает, когда учетная запись не имеет привилегий локального администратора на компьютере, где запущен сервис DeviceLock.

Загрузка / Сохранение / Экспорт

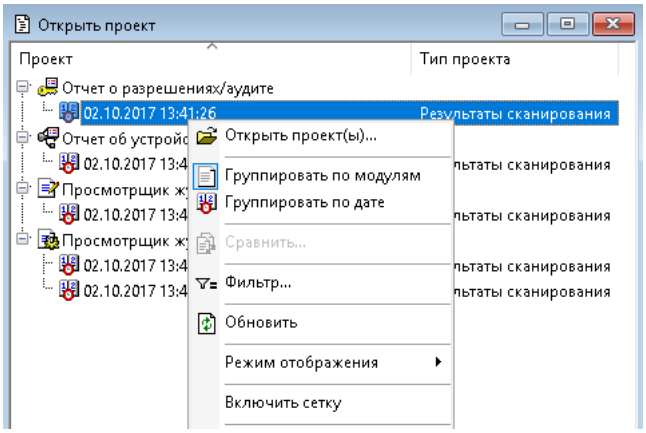
DeviceLock Enterprise Manager может сохранять всю информацию, полученную от модулей. Данные сохраняются во внешних файлах и по запросу могут быть загружены в DeviceLock Enterprise Manager.

Существует три варианта сохранения и загрузки данных:

1. Наиболее удобный способ хранения полученной информации - в виде проекта. DeviceLock Enterprise Manager сохраняет каждое окно с информацией в отдельном файле и помещает эти файлы в папку ***Project***. Имена файлов проекта формируются автоматически и зависят от названия модуля, даты и времени начала сканирования.

   Чтобы сохранить данные в виде проекта, вы можете выбрать команду **Сохранить проект** из меню **Файл** или нажать на соответствующую кнопку на панели инструментов.

   Для загрузки сохраненного проекта вы можете выбрать пункт **Открыть проект** из меню **Файл**. Окно **Открыть проект** имеет собственную панель инструментов и контекстное меню.



   Можно сгруппировать сохраненные проекты по датам, когда выполнялось сканирование, и по типу информации, содержащейся в них. Выберите пункт **Группировать по модулям** или **Группировать по дате** из контекстного меню или нажмите соответствующую кнопку на панели инструментов **Проект**.

   Чтобы открыть сохраненный проект, выберите его из списка и нажмите кнопку **Открыть проект** на панели инструментов **Проект**. Используя клавиши Ctrl и/или Shift, вы можете открыть одновременно несколько проектов.

2. Другой способ сохранения полученной информации в DeviceLock Enterprise Manager - с помощью команды **Сохранить как** из меню **Файл**. Этот способ позволяет вам сохранить файл в формате ANM в любом месте вашего диска или на любом ином устройстве и с любым именем.

   Для загрузки сохраненного файла выберите команду **Открыть** из меню **Файл** или нажмите соответствующую кнопку на основной панели инструментов. Затем укажите требуемый. Загрузить можно будет лишь файлы в формате ANM.

3. Если требуется передать полученную информацию во внешнее приложение, можно экспортировать данные во внешний файл и затем импортировать их в это приложение. Для экспорта данных во внешний файл выберите команду **Сохранить как** из меню **Файл** и затем выберите тип файла из списка. DeviceLock Enterprise Manager поддерживает экспорт в MS Excel (если он установлен на локальном компьютере) и в два текстовых формата - Tab Delimited (TXT) и Comma Delimited (CSV).

   Если вы экспортируете информацию во внешний файл, вы не сможете загрузить ее обратно, поскольку DeviceLock Enterprise Manager может открывать и загружать файлы только собственного формата (ANM). Экспорт во внешний файл предназначен для обмена данными между DeviceLock Enterprise Manager и другими приложениями.

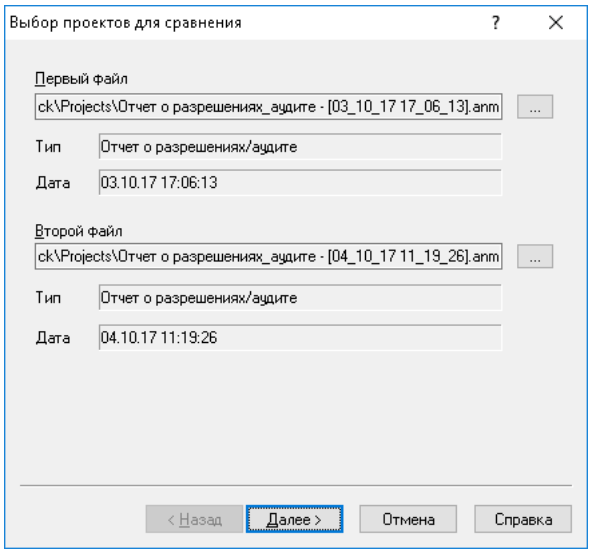
Сравнение данных

DeviceLock Enterprise Manager позволяет отслеживать изменения на сетевых компьютерах, сравнивая два предварительно сохраненных проекта. Сравнение изменений очень важно, когда выполняется управление большим количеством компьютеров одной сети.

DeviceLock Enterprise Manager предоставляет удобный и простой в использовании мастер сравнения двух ANM-файлов. Чтобы открыть этот мастер сравнения, выберите подпункт **Сравнить** из меню **Файл**.

Ниже приведены три простых шага, которые позволят вам сравнить два файла, используя мастер сравнения:

1. Первый шаг - выбор файлов для сравнения.

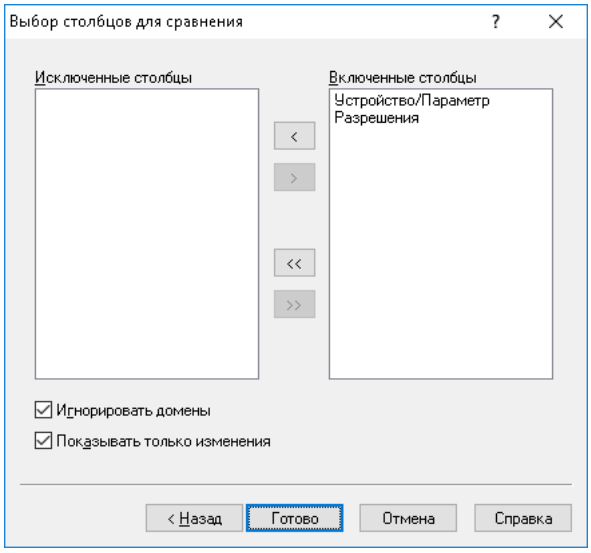


   Выберите первый файл, затем второй нажатием соответствующих кнопок ...

   Помните, что вы можете сравнивать файлы только одного и того же типа. Например, вы не можете сравнивать информацию, полученную от модуля **Отчет о разрешениях/аудите** с информацией, полученной от модуля **Отчет об устройствах PnP**.

   После выбора двух файлов, нажмите кнопку **Далее** для перехода к следующей странице мастера сравнения.

2. Второй шаг - выбор столбцов, по которым требуется выполнить сравнение.



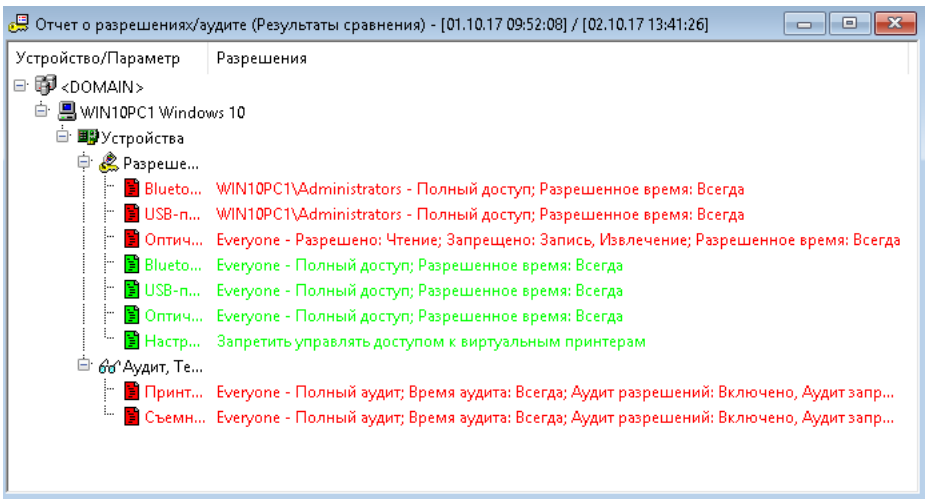
DeviceLock Enterprise Manager сравнивает только те столбцы, которые были выбраны на этом шаге. Если вам необходимо исключить один столбец из процесса сравнения, вам необходимо переместить его из списка **Включенные столбцы** в список **Исключенные столбцы**. Исключенные столбцы будут видны в результате сравнения, но их значения игнорируются и не оказывают влияния на результат.

По умолчанию, результат сравнения будет содержать только те записи, которые имеют различия в выбранных для сравнения файлах. Чтобы увидеть все записи (включая одинаковые), снимите флажок **Показывать только изменения**.

Для включения имен доменов в процесс сравнения, снимите флажок **Игнорировать домены**. Когда этот флажок установлен, DeviceLock Enterprise Manager игнорирует домены и сравнивает только компьютеры и информацию, которую они содержат.

3. Третий и заключительный шаг - запуск процесса сравнения. Нажмите кнопку **Готово** для выполнения сравнения двух выбранных файлов.

   DeviceLock Enterprise Manager отобразит результат сравнения в отдельном окне в виде дерева в точности, как отображается информация, полученная от модулей в процессе сканирования.



Алгоритм сравнения очень прост и эффективен:

1. Если флажок **Игнорировать домены** снят, программа определяет количество доменов в двух выбранных файлах и пытается найти каждый из них как в старом, так и в новом файле.

   Если домен имеется в старом файле, но отсутствует в новом, программа вставляет отсутствующий домен (включая все входящие в этот домен компьютеры и информацию, которая для них имеется) в результат сравнения и отображает все эти записи красным цветом.

   Если домен отсутствует в старом файле, но имеется в новом, программа вставляет отсутствующий домен (включая все входящие в этот домен компьютеры и информацию, которая для них имеется) в результат сравнения и отображает все эти записи зеленым.

   Если домен существует в обоих файлах, программа перебирает все входящие в этот домен компьютеры (см. ниже).

2. Если флажок **Игнорировать домены** установлен, программа будет игнорировать домены и переберет все компьютеры в обоих выбранных файлах, после чего попытается найти каждый компьютер, как в старом, так и в новом файле.

   Если компьютер имеется в старом файле, но отсутствует в новом, программа вставит отсутствующий компьютер вместе со всей его информацией в результат сравнения и отметит все записи красным.

   Если компьютер не существует в старом файле, но присутствует в новом, программа вставит отсутствующий компьютер вместе со всей его информацией в результат сравнения и отметит все записи зеленым цветом.

   Если компьютер имеется в обоих файлах, программа перебирает всю относящуюся к нему информацию (см. ниже).

3. Программа перебирает всю относящуюся к компьютеру информацию и пытается найти одинаковые записи в обоих файлах.

   Если запись имеется в старом файле и отсутствует в новом, программа вставит отсутствующую запись в результат сравнения и выделит ее красным цветом.

   Если запись отсутствует в старом файле, но присутствует в новом, программа вставит отсутствующую запись в результат сравнения и выделит ее зеленым цветом.

   Если запись имеется в обоих файлах, программа запустит процедуру сравнения каждого входящего в эту запись столбца:

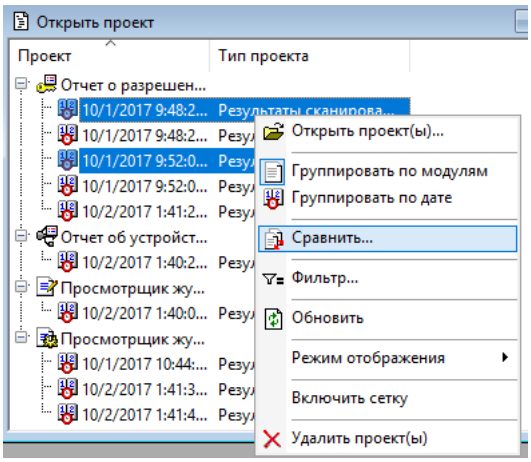
   - Если значение столбца для файлов различны, программа вставит обе записи в результат сравнения. Запись из нового файла будет размещена после записи из старого файла.

     Содержимое столбца, принадлежащее старой записи, будет выделено красным цветом. Содержимое столбца, принадлежащее новой записи, будет выделено зеленым. Содержимое всех, не включенных в процесс сравнения столбцов, выводится цветом по умолчанию.

   - Если записи всех столбцов обоих файлов имеют одинаковые значения, программа либо пропустит эту запись (установлен флажок **Показывать только изменения**), либо вставит запись в результат сравнения, используя цвет по умолчанию (флажок **Показывать только изменения** снят).

Если требуется сравнить два файла, которые были сохранены как проекты, то удобно будет использовать специальную возможность окна **Открыть проект**.

Выберите команду **Открыть проект** из меню **Файл**, выделите два проекта, которые нужно сравнить (используйте Ctrl и/или Shift для одновременного выделения двух проектов), а затем выберите пункт **Сравнить** из контекстного меню или нажмите на соответствующую кнопку на панели инструментов **Проект**.

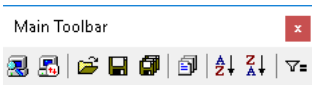


Примечание: Можно выбрать только два проекта для сравнения, и оба проекта должны быть одного и того же типа.

DeviceLock Enterprise Manager предоставляет панель инструментов для навигации по результатам сравнения:

Нажимайте левую или среднюю кнопку на этой панели для перехода к предыдущему или последующему изменению в результатах сравнения. Самая правая кнопка открывает легенду отображения результатов сравнения.

Результаты сравнения могут быть сохранены во внешнем файле формата ANM или экспортированы в MS Excel или текстовый файл (TXT или CSV). Выберите команду **Сохранить как** из меню **Файл** или нажмите соответствующую кнопку на основной панели инструментов для сохранения или экспорта результатов сравнения.

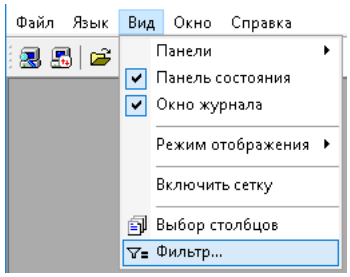


Как и любые другие файлы, сохраненные результаты могут быть открыты и загружены обратно в DeviceLock Enterprise Manager. Загрузить предварительно сохраненные результаты сравнения можно с помощью команды **Открыть** из меню **Файл** или соответствующей кнопки на основной панели инструментов. Затем выберите требуемый файл. Допускается загрузка только файлов формата ANM.

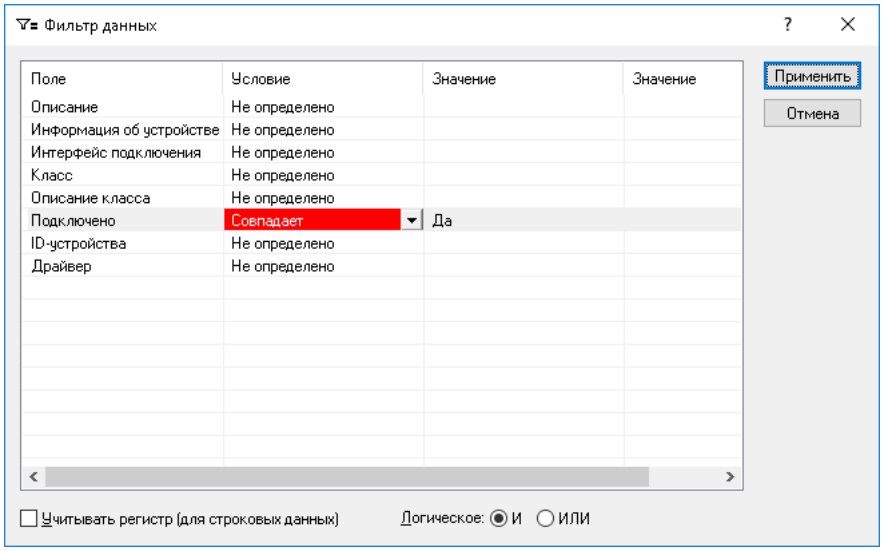
Фильтрация данных

DeviceLock Enterprise Manager предоставляет очень мощную функцию фильтрации данных, позволяющую вам ограничить результаты сканирования и/или сравнения только теми данными, которые необходимы.

Чтобы открыть диалоговое окно **Фильтр данных**, можно выбрать команду **Фильтр** из меню **Вид** или нажать на соответствующую кнопку на основной панели инструментов.



Примечание: Столбец **Поле** в диалоговом окне **Фильтр данных** отображает все поля, доступные в результатах сканирования или сравнения, по значению которых можно задать фильтр.



- Столбец **Поле** отображает все поля, доступные в результатах сканирования или сравнения, по значению которых можно задать фильтр. Можно использовать логику "И-ИЛИ" для всех полей:
  - **И** - Включает в результат только те записи, которые удовлетворяют всем заданными условиями. Например, Процесс = `"explorer.exe"` И PID = `3764` возвратит все данные, в которых значение Процесс равно `"explorer.exe"`, а PID равен `3764`. Результат не будет включать в себя данные, в которых значение поля Процесс равно `"explorer.exe"`, а PID не равен `3764`, или где PID равен `3764`, но значение поля Процесс не равно `"explorer.exe"`.
  - **ИЛИ** - Включает в результат записи, которые удовлетворяют хотя бы одному заданному условию. Например, Процесс = `"explorer.exe"` ИЛИ PID = `3764` возвратит все данные, в которых верно одно или оба условия, где Процесс = `"explorer.exe"` (не важно, какое значение при этом имеет PID) или где PID равен `3764` (не важно, какое значение имеет Процесс).

- Столбец **Условие** содержит список логических операций, которые могут быть применены к выбранному полю. Вы можете выбрать только одну логическую операцию для каждого поля. DeviceLock Enterprise Manager поддерживает две группы логических операций, для строковых данных и для не строковых данных.

  Логические операции, которые могут быть выполнены над строковыми данными (сравниваемое значение (аргумент) также должно быть строковым, например "explorer.exe"):

  - **Совпадает** - Отбираются только те данные, значения полей которых полностью соответствуют сравниваемой строке.
  - **Включает** - Обираются только те данные, значения полей которых входят (содержатся) в сравниваемую строку.
  - **Не совпадает** - Отбираются только те данные, значения полей которых отличны от сравниваемой строки.
  - **Не включает** - Отбираются только те данные, значения полей которых не входят (не содержатся) в сравниваемую строку.
  - **Пусто** - Отбираются только те данные, поля которых содержат пустую строку.
  - **Не пусто** - Отбираются только те данные, поля которых не пустые.
  - **Регулярное выражение** - Отбираются только те данные, строки в полях которых удовлетворяют регулярному выражению. Регулярное выражение может содержать символы подстановки (например, "expl*e?").

  Если требуется учитывать регистр букв в строке (например, чтобы "Explorer.exe" отличался от "explorer.exe"), установите флажок **Учитывать регистр**. В противном случае регистр букв игнорируется (например, строки "Explorer.exe" и "explorer.exe" считаются одинаковыми).

  Логические операции, выполняемые над не строковыми данными:

  - **Равно (=)** - Отбираются данные, в которых значение сравниваемого поля равно заданному значению (например, PID = 3764).
  - **Больше (>)** - Отбираются данные, значение сравниваемого поля которых больше, чем заданное значение (например, PID > 4).
  - **Меньше (<)** - Отбираются данные, значение сравниваемого поля которых меньше, чем заданное значение (например, PID < 4).
  - **Не равно (!=)** - Отбираются данные, значение сравниваемого поля которых не равно заданному значению (например, PID != 0).
  - **Внутри интервала (in)** - Отбираются данные, значение сравниваемого поля которых находится между двумя заданными значениями (например, PID in 3000-4000).
  - **Вне интервала (out)** - Отбираются данные, значение сравниваемого поля которых находится вне региона двух заданных значений (например, PID out 3000-4000).
  - **Регулярное выражение** - Отбираются только те данные, значение полей которых удовлетворяют регулярному выражению. Регулярное выражение может содержать символы подстановки (например, 3*1?9).

  Если вы не хотите выполнять логическую операцию для поля, выберите в списке логических операций пункт **Не определено**.

- Столбец **Значение** содержит заданные пользователем аргументы. Второй столбец **Значение** используется только для случаев, если выбраны логические операции **Внутри интервала (in)** или **Вне интервала (out)**. Для всех остальных логических операций требуется только первый столбец **Значение**.

После того, как выражение для фильтра определено, нажмите кнопку **Применить**.

Результат фильтрации можно сохранить во внешнем файле ANM, либо экспортировать его в текстовый файл (TXT и CSV) или MS Excel. Выберите команду **Сохранить как** из меню **Файл** или нажмите на соответствующую кнопку на основной панели инструментов для сохранения или экспорта результатов.

Как и любые другие файлы, сохраненные результаты могут быть открыты и загружены обратно в DeviceLock Enterprise Manager. Для того чтобы загрузить предварительно сохраненные результаты фильтрации, можно выбрать команду **Открыть** из меню **Файл** или нажать соответствующую кнопку на основной панели инструментов. Затем выберите требуемый файл. Допускается загрузка только файлов формата ANM.

Сертификаты DeviceLock

Сертификат состоит из двух ключей (ключевой пары): секретного ключа и открытого ключа.

- Секретный ключ должен храниться на компьютере администратора, и только администратор должен иметь доступ к нему. Секретный ключ также может быть установлен на серверах DeviceLock Enterprise Server и DeviceLock Content Security Server.

  Примечание: Убедитесь, что обычные пользователи не могут получить доступ к секретному ключу.

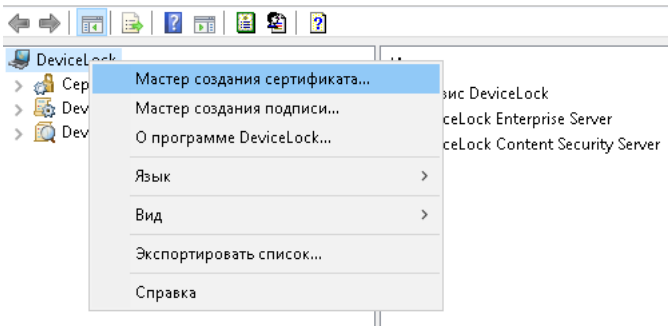
- Открытый ключ устанавливается на все компьютеры, где работает сервис DeviceLock. Если открытый ключ не предустановлен на компьютере пользователя, недоступными окажутся функция Временный белый список и аутентификация на основе сертификата DeviceLock для DeviceLock Enterprise Server и DeviceLock Discovery.

Создание сертификата

Прежде всего надо создать сертификат, используя мастер создания сертификата, установленный вместе с консолями управления DeviceLock.

Мы рекомендуем создать только один сертификат и установить его открытый ключ на все пользовательские компьютеры. Генерация и установка нового сертификата необходима только в случае компрометации секретного ключа или при его утере.

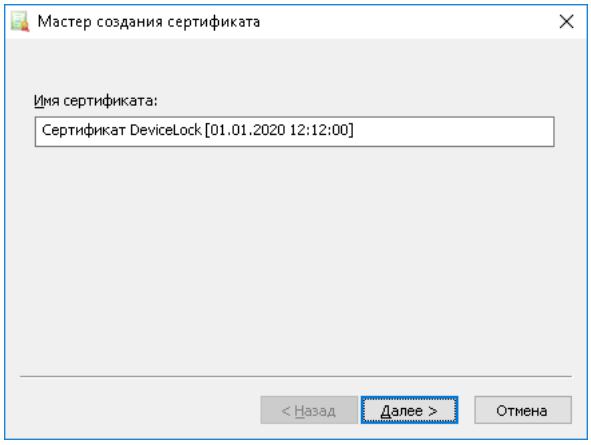
Чтобы запустить мастер создания сертификата, выберите **Мастер создания сертификата** из меню **Файл** в приложении DeviceLock Enterprise Manager. Чтобы запустить мастер создания сертификата из консоли DeviceLock Management Console или DeviceLock Group Policy Manager, щелкните правой кнопкой мыши и выберите соответствующий пункт в контекстном меню.



Мастер создания сертификата запустится автоматически при установке консолей управления DeviceLock на компьютере администратора без сертификата DeviceLock.

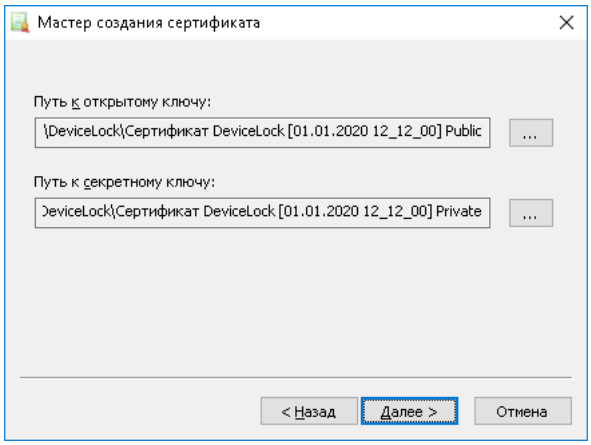
Для создания пары ключей нужно выполнить два простых шага:

1. Задать имя сертификата.



Мастер создания сертификата автоматически создает имя, основанное на текущей дате и времени, и позволяет ввести любое иное имя.

2. Задать путь и имена файлов для секретного и открытого ключей.



Как только сертификат будет создан, можно приступать к установке открытого ключа на пользовательские компьютеры.

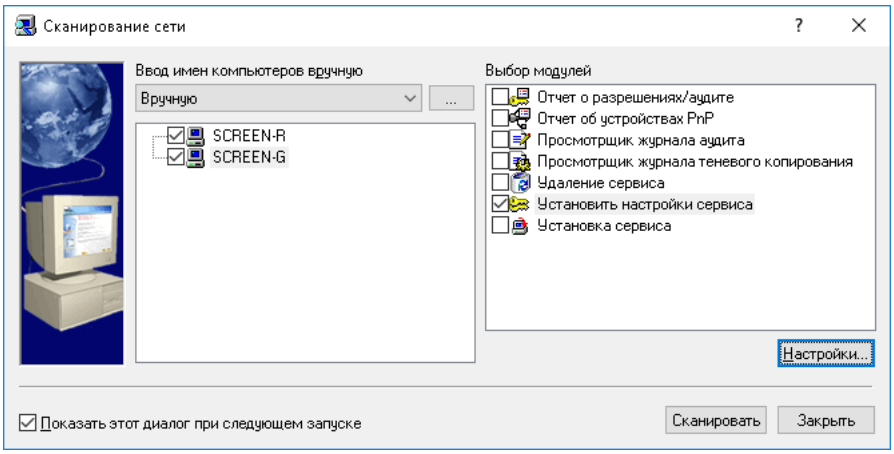
Внимание: Вновь созданный сертификат не устанавливается автоматически на компьютеры с помощью мастера создания сертификата. Его требуется установить вручную, используя консоль управления DeviceLock.

Установка и удаление сертификата

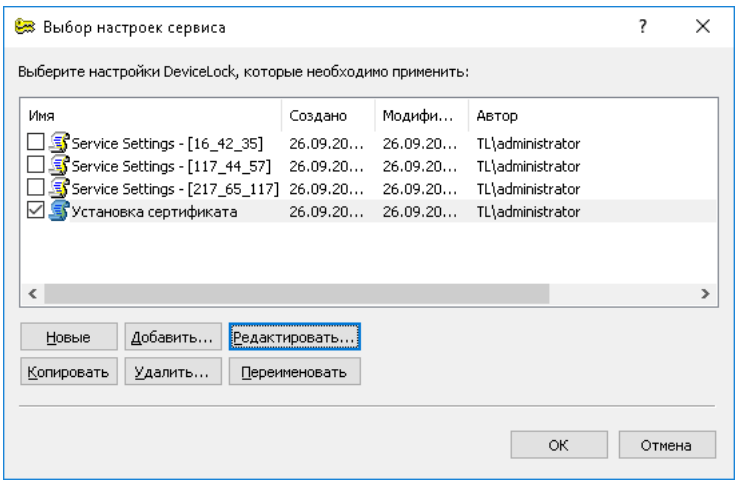
Чтобы установить или удалить открытый ключ с пользовательских компьютеров, можно использовать любую консоль управления DeviceLock.

Использование DeviceLock Enterprise Manager

1. В диалоге **Сканирование сети** выберите компьютеры для установки или удаления открытого ключа, затем выберите модуль **Установить настройки** сервиса.



2. Нажмите кнопку **Настройки**, чтобы открыть диалог с настройками.

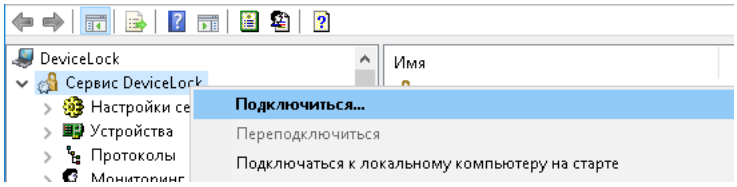


3. Чтобы задать политику, в которой будет устанавливаться или удаляться сертификат, создайте новый файл настроек сервиса DeviceLock или используйте один из существующих. Выберите файл в списке и затем нажмите кнопку **Редактировать** для редактирования политики, как это описано ниже в разделе Использование консоли DeviceLock Management Console, DeviceLock Group Policy Manager или DeviceLock Service Settings Editor. Когда редактирование политики будет закончено, отметьте файл в списке, установив флажок рядом с его именем.

4. Нажмите **OK**, чтобы закрыть диалог с настройками и затем нажмите кнопку **Сканировать** в диалоговом окне **Сканирование сети**, чтобы начать процесс установки или удаления ключа.

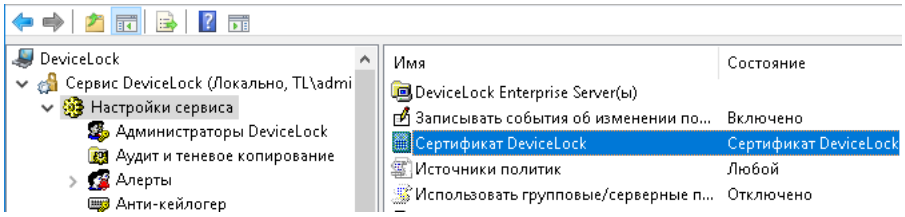
Использование консоли DeviceLock Management Console, DeviceLock Group Policy Manager или DeviceLock Service Settings Editor

1. При использовании консоли DeviceLock Management Console необходимо подключиться к компьютеру с запущенным сервисом DeviceLock. Используйте контекстное меню, доступное по нажатию правой кнопки мыши.

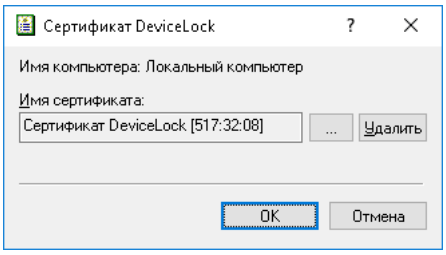


   При использовании консоли DeviceLock Group Policy Manager подключаться к клиентским компьютерам не требуется, т.к. эта консоль работает с объектом групповой политики, а не с отдельным компьютером. Также не требуется подключаться к клиентским компьютерам при использовании консоли DeviceLock Service Settings Editor для редактирования политики во внешнем файле настроек сервиса DeviceLock.

2. Выберите раздел **Настройки сервиса** из дерева консоли.



3. На панели сведений консоли дважды щелкните элемент **Сертификат DeviceLock**, чтобы открыть диалог с настройками.



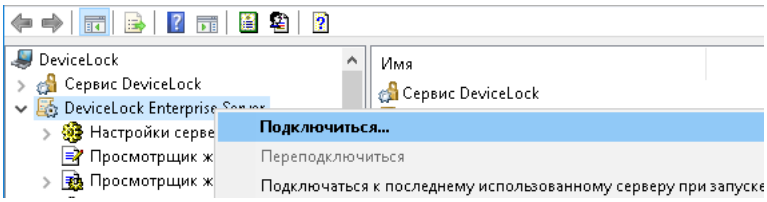
4. Укажите файл с открытым ключом в поле **Имя сертификата**, если требуется установить сертификат. Нажмите кнопку ..., чтобы открыть для диалог выбора файла.

   Для удаления открытого ключа используйте кнопку **Удалить**.

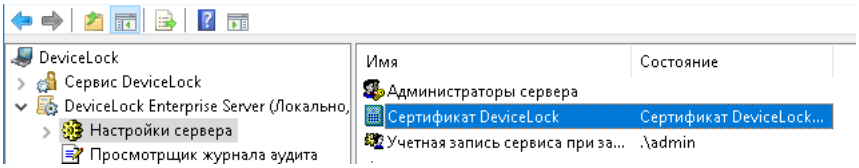
5. Нажмите **OK**, чтобы закрыть диалог и применить настройки.

Чтобы установить или удалить секретный ключ на сервере DeviceLock Enterprise Server или DeviceLock Content Security Server, следует использовать консоль DeviceLock Management Console:

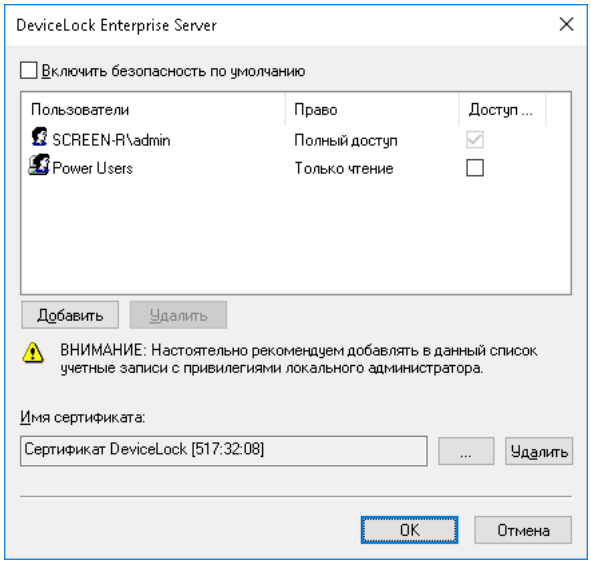
1. Подключите консоль к компьютеру, на котором работает DeviceLock Enterprise Server или DeviceLock Content Security Server. Используйте команду **Подключиться** из контекстного меню, доступного по нажатию правой кнопки мыши.



2. Выберите раздел **Настройки сервера** в дереве консоли.



3. На панели сведений консоли дважды щелкните элемент **Сертификат DeviceLock**, чтобы открыть диалоговое окно с настройками.



4. Укажите файл с секретным ключом в поле **Имя сертификата**. Нажмите кнопку ..., чтобы открыть диалоговое окно для выбора файла, содержащего секретный ключ сертификата.

   Для удаления секретного ключа используйте кнопку **Удалить**.

5. Нажмите **OK**, чтобы закрыть диалог и применить настройки.

Подробнее об установке секретного ключа см. в описании параметра Имя сертификата для DeviceLock Enterprise Server (раздел Установка DeviceLock Enterprise Server) и в описании параметра Имя сертификата для DeviceLock Content Security Server (раздел Установка DeviceLock Content Security Server).

Мастер создания подписи

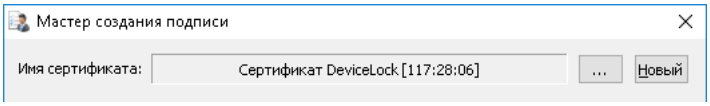
Мастер создания подписи - это инструмент, позволяющий предоставлять пользователям временный доступ к запрошенным устройствам, а также подписывать файлы с настройками сервиса DeviceLock, созданные в консоли DeviceLock Management Console, DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

Чтобы запустить мастер создания подписи, выберите **Мастер создания подписи** из меню **Файл** в консоли DeviceLock Enterprise Manager или из контекстного меню в консоли DeviceLock Management Console или DeviceLock Service Settings Editor.

Прежде всего нужно загрузить секретный (закрытый) ключ сертификата DeviceLock.

Мастер создания подписи должен использовать секретный ключ, который принадлежит тому же сертификату, что и открытый ключ, установленный на пользовательском компьютере.

По умолчанию мастер создания подписи автоматически загружает последний использованный сертификат. Загрузить другой сертификат можно, нажав кнопку ... и выбрав файл с секретным ключом.

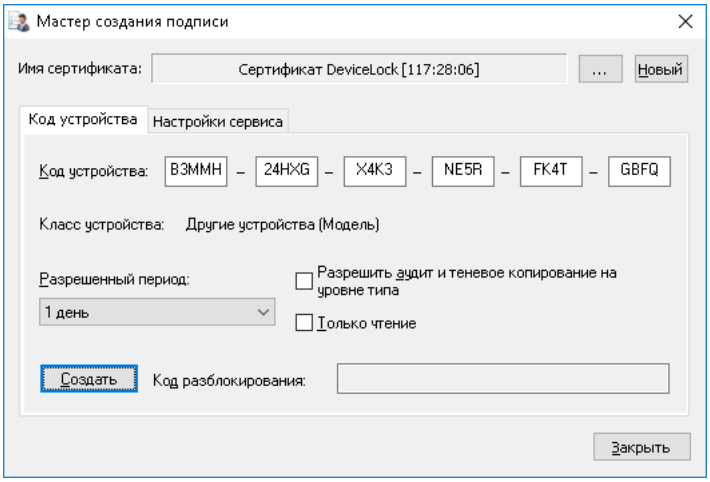


Для создания нового сертификата используется мастер создания сертификата (см. Создание сертификата), который можно запустить непосредственно из мастера создания подписи. Для этого нажмите кнопку **Новый**. После создания нового сертификата его открытый ключ нужно будет установить на пользовательских компьютерах.

Дальнейшие шаги зависят от задачи, которую требуется выполнить: создать разблокирующий код (см. Код устройства) или подписать файл настроек сервиса DeviceLock (см. Настройки сервиса).

Код устройства

Чтобы предоставить пользователю временный доступ к устройству, администратор должен создать **код разблокирования** в ответ на присланный ему **код устройства**. Подробнее о коде устройства см. в разделе Временный белый список данного руководства.



Чтобы создать код разблокирования, следует выполнить четыре шага:

1. Загрузить секретный ключ сертификата DeviceLock, как описано выше.
2. Ввести присланный пользователем код устройства.

   После того как будет введен корректный код устройства, в поле **Класс устройства** можно увидеть класс устройства, к которому пользователь хочет получить доступ. Информация о классе устройства помогает проконтролировать, какое устройство пользователь намерен использовать. Если, к примеру, пользователь сообщает администратору, что он намерен использовать USB-сканер, а на самом деле пытается получить доступ к флеш-диску, администратор сможет увидеть это несоответствие.

   В круглых скобках рядом с классом устройства указывается, может ли запрашиваемое устройство быть авторизовано как уникальное устройство с серийным номером либо оно может быть авторизовано лишь как модель. Если устройство авторизуется как модель, то пользователь получит доступ ко всем устройствам этой модели. Подробнее см. в разделе Белый список USB-устройств (обычный профиль) данного руководства.
3. Выбрать период, в течение которого устройство будет доступно пользователю. В поле **Разрешенный период** можно выбрать одно из следующих значений: 5, 15, 30, 60 минут; 5 часов; 1 или 2 дня; 1 или 2 недели; 1 месяц; пока устройство не будет отключено или пока текущий пользователь не завершит свою сессию (не выйдет из системы).

   Если выбрать фиксированное время (например, 10 минут), то пользователь получит доступ к устройству только на этот период. По истечении разрешенного времени доступ к устройству будет запрещен. При этом неважно, что именно пользователь делает с этим устройством; даже если он все еще копирует файлы на USB-диск или печатает документ на USB-принтере, все операции будут прерваны.

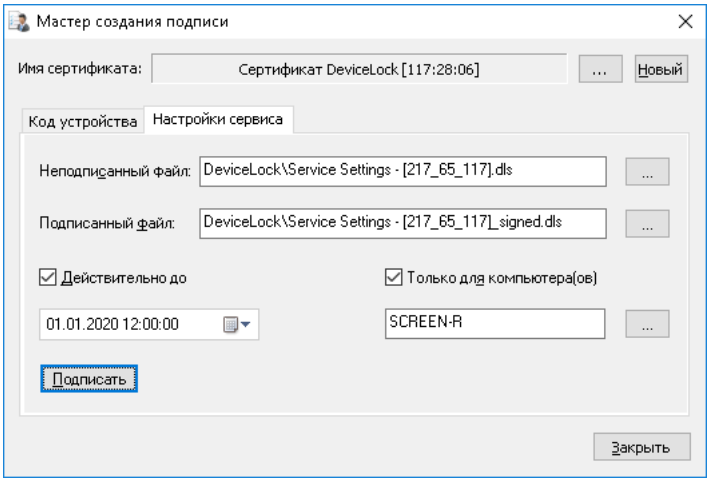
   Чтобы разрешить пользователю использовать устройство без ограничения времени, выберите опцию **до извлечения** в поле **Разрешенный период**. Пользователь получит доступ к устройству до тех пор, пока оно будет подключено к порту. Как только пользователь отключит это устройство, доступ к нему будет запрещен.
4. Нажать кнопку **Создать**, чтобы создать код разблокирования. Передайте этот код пользователю по телефону или любым другим способом.

   Время создания кода зависит от мощности компьютера и может составить несколько секунд.

Настройки сервиса

Для предотвращения несанкционированных изменений файла с настройками сервиса DeviceLock его можно подписать при помощи цифровой подписи.

Позже этот файл может быть отправлен пользователям, чьи компьютеры не подключены к сети и находятся вне досягаемости консолей управления.



Подписывание файла осуществляется в шесть простых шагов:

1. Загрузите секретный ключ сертификата DeviceLock, как описано выше.
2. Загрузите файл с настройками, который требуется подписать.

   Полный путь к файлу должен быть указан в поле **Неподписанный файл**. Нажмите кнопку ..., чтобы открыть диалог для выбора файла.

   Файл с настройками сервиса DeviceLock может быть создан при помощи команды "Сохранить настройки сервиса" из контекстного меню консоли DeviceLock Management Console, DeviceLock Group Policy Manager или DeviceLock Service Settings Editor.
3. В поле **Подписанный файл** укажите путь к результирующему файлу с подписью. Нажмите кнопку ..., чтобы выбрать папку для сохранения этого файла.
4. Решите, должен ли результирующий файл содержать информацию о сроке годности.

   Чтобы позволить пользователям импортировать настройки из этого файла без каких-либо ограничений по времени, снимите флажок **Действительно до**.

   Если флажок **Действительно до** установлен и заданы дата и время, то информация о сроке годности файла будет записана в результирующий файл и пользователи смогут импортировать настройки из этого файла только до указанной даты/времени.

   Данный флажок имеет силу только когда пользователи импортируют настройки сервиса DeviceLock через приложение **DeviceLock** из Панели управления Windows. Когда файл с настройками загружается при помощи команды **Загрузить настройки сервиса** из контекстного меню консоли DeviceLock Management Console или DeviceLock Group Policy Manager, информация о сроке годности файла игнорируется.
5. Решите, должен ли результирующий файл быть привязан к определенному компьютеру, или следует разрешить его использование на любом компьютере.

   Чтобы позволить пользователям импортировать настройки из этого файла на любых компьютерах, снимите флажок **Только для компьютера(ов)**.

Если флажок **Только для компьютера(ов)** установлен и указано имя компьютера, то пользователи смогут импортировать настройки из этого файла только на указанном компьютере. Используя точку с запятой (;) в качестве разделителя, можно указать несколько имен компьютеров, что позволит импортировать результирующий файл на любом из этих компьютеров.

> **Примечание:** В этом параметре нельзя использовать IP-адрес компьютера. Требуется указывать именно имя компьютера, в точности как оно отображается в программе **Система** из панели управления Windows.
>
> На компьютерах Mac должно использоваться имя, выводимое командой **hostname**. То же самое имя компьютера можно посмотреть в панели **Системные настройки** > **Общий доступ**.

Можно загрузить заранее подготовленный список компьютеров из внешнего текстового файла. Чтобы открыть внешний файл, нажмите кнопку ... . Текстовый файл должен содержать имена компьютеров, каждое из которых должно быть записано на отдельной строке.

Данный флажок имеет силу только когда пользователи импортируют настройки сервиса DeviceLock через приложение **DeviceLock** из панели управления Windows. Когда файл с настройками загружается при помощи команды **Загрузить настройки сервиса** из контекстного меню консоли DeviceLock Management Console или DeviceLock Group Policy Manager, информация о привязке к компьютеру игнорируется.

6. Нажмите кнопку **Подписать**, чтобы создать подписанный файл с настройками сервиса DeviceLock. Затем передайте полученный файл пользователю.

   Процесс создания цифровой подписи - это ресурсоемкая операция. Время создания подписи зависит от мощности процессора и может составить несколько секунд.

Параметры командной строки для подписи файла настроек

Подписать файл настроек можно, используя `DLTempAccessAdmin.exe` в командной строке. Файл `DLTempAccessAdmin.exe` находится в папке установки DeviceLock:

- `%ProgramFiles%\DeviceLock\` по умолчанию на 32-разрядной ОС.
- `%ProgramFiles(x86)%\DeviceLock\` по умолчанию на 64-разрядной ОС.

Чтобы подписать файл настроек, в командной строке перейдите в папку установки DeviceLock и используйте следующий синтаксис:

```
DLTempAccessAdmin.exe -s <in-file> -d <out-file> [-c <key-file>]
```

Значения параметров в этом синтаксисе:

- `<in-file>` - Путь и имя файла настроек, который требуется подписать.
- `<out-file>` - Путь и имя файла выходного подписанного файла настроек.
- `<key-file>` - Путь и имя файла, содержащего секретный ключ сертификата DeviceLock.

Пример:

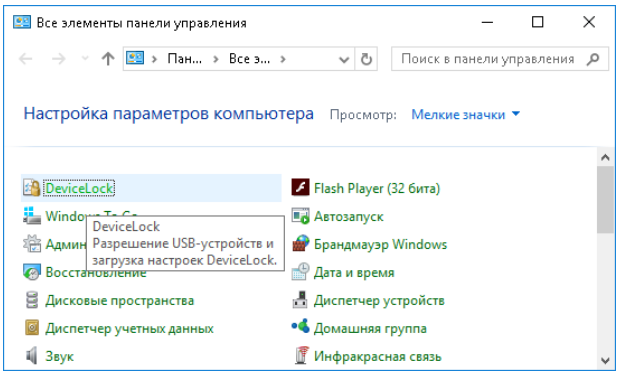
```
DLTempAccessAdmin.exe -s c:\temp\src.dls -d c:\temp\signed.dls -c c:\temp\private
```

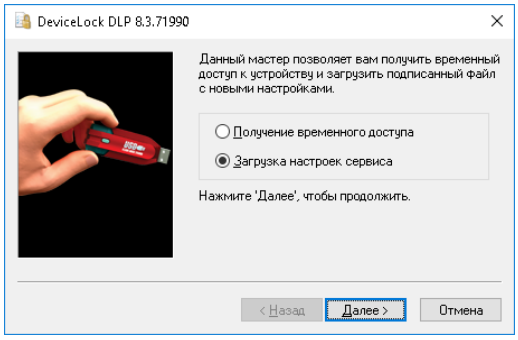
Если параметр `-c <key-file>` не указан, используется ключ, который ранее использовался в мастере создания подписи. Если этот параметр указан, заданный им ключ запоминается и по умолчанию используется в последующих операциях создания подписи.

Если путь или имя файла содержит пробелы, значение параметра необходимо заключить в кавычки, например: `-s "c:\temp\my settings"`.

Загрузка подписанного файла настроек на Windows

Чтобы применить настройки сервиса DeviceLock из подписанного файла, необходимо запустить приложение **DeviceLock** из панели управления Windows и выбрать опцию **Загрузка настроек сервиса**.



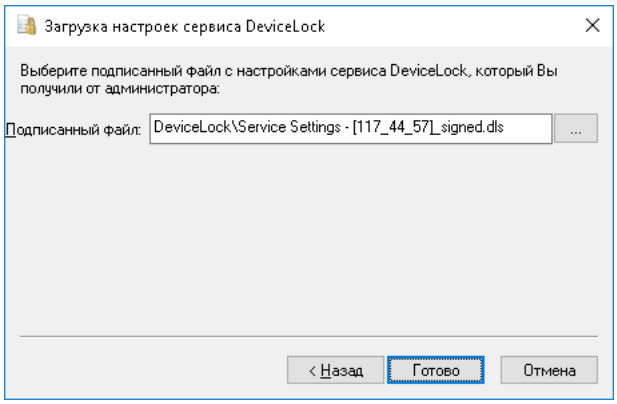


Примечание:

- Для доступа к приложению DeviceLock необходимо выбрать режим просмотра “Мелкие значки” в панели управления.
- В заголовке окна приложения отображаются версия и номер сборки DeviceLock.
- Запуск приложения DeviceLock из панели управления Windows может завершиться ошибкой “Сертификат не установлен.” Для устранения этой проблемы на клиентском компьютере необходимо установить открытый ключ сертификата DeviceLock. Инструкции см. в разделе Установка и удаление сертификата.

Чтобы загрузить настройки из подписанного файла, пользователю требуется выполнить два простых действия:

1. Ввести полный путь и имя файла в поле **Подписанный файл**. Можно нажать кнопку ... для выбора файла.



2. Нажать кнопку **Готово**.

Если цифровая подпись файла верна, то новые настройки будут немедленно загружены в сервис DeviceLock. Появится следующее сообщение: “Файл успешно загружен.”

Пользователь может также загрузить настройки сервиса DeviceLock из подписанного файла используя командную строку:

```
DLTempAccess.cpl -s <путь к подписанному файлу>
```

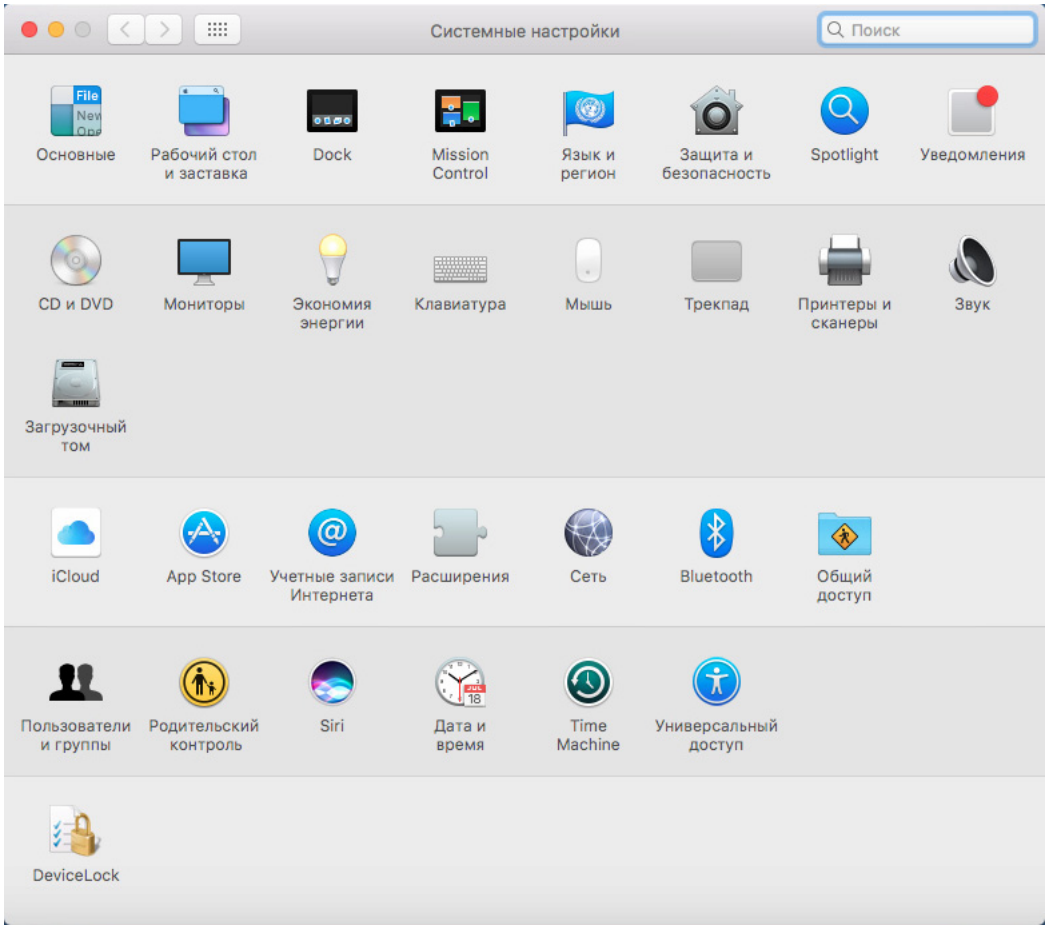
Здесь `<путь к подписанному файлу>` - это полный путь к подписанному файлу с настройками сервиса DeviceLock. Пример:

```
DLTempAccess.cpl -s "C:\Program Files\DeviceLock\settings_signed.dls"
```

Все успешные попытки загрузить настройки из файла протоколируются, если включен параметр Записывать события об изменении политики и старте/остановке сервиса (см. раздел Настройки сервиса).

Загрузка подписанного файла настроек на Mac

Сервис DeviceLock для Mac устанавливает собственное приложение в панель системных настроек компьютера: **Системные настройки** > **DeviceLock**.



Чтобы загрузить настройки из подписанного файла, пользователю Mac требуется запустить приложение **DeviceLock** из панели системных настроек компьютера, нажать кнопку **Далее** в появившемся диалоговом окне и затем выполнить следующие действия:

1. Ввести путь и имя подписанного файл с настройками сервиса DeviceLock. Для выбора файла можно использовать кнопку рядом с полем ввода.
2. Нажать кнопку **Применить**.

Если цифровая подпись файла с настройками проходит проверку, новые настройки будут немедленно загружены в сервис DeviceLock. Появится следующее сообщение: “Файл успешно загружен.”

Загрузить настройки сервиса DeviceLock из подписанного файла можно также с помощью командной строки:

```
/Library/DeviceLockAgent/Utilities/DLAgentControl importdls <путь к файлу>
```

Здесь `<путь к файлу>` - полный путь к подписанному файлу с настройками сервиса DeviceLock.

Пример:

```
/Library/DeviceLockAgent/Utilities/DLAgentControl importdls
/home/user/Desktop/settings_signed.dls
```

Примечание: Администратор DeviceLock, не обладающий правами администратора компьютера, не сможет получить доступ к папке /Library/DeviceLockAgent/Utilities. Во избежание такой ситуации можно предварительно скопировать приложение DLAgentControl в другую папку. Это приложение доступно также в папке Utilities на установочном образе .dmg.

Все успешные попытки загрузить настройки из файла протоколируются, если включен параметр Записывать события об изменении политики и старте/остановке сервиса (см. раздел Настройки сервиса).

4

Сервис DeviceLock

В этой главе:

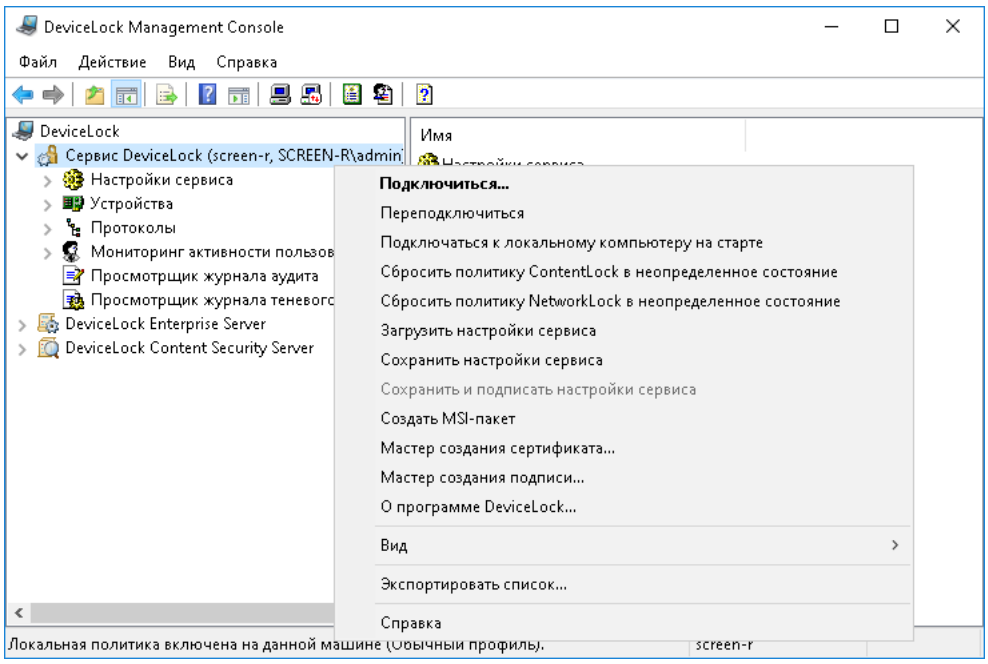
Управление сервисом DeviceLock для Windows

Управление сервисом DeviceLock для Mac

Управление сервисом DeviceLock для Windows

В дереве консоли раскройте узел **Сервис DeviceLock**, чтобы получить доступ ко всем функциям и параметрам сервиса.

Внимание: Для просмотра или изменения любых параметров сервиса в консоли DeviceLock Management Console необходимо сначала подключить ее к компьютеру, на котором работает сервис DeviceLock. Подробнее см. в разделе Подключение к компьютеру.



Контекстное меню узла **Сервис DeviceLock** содержит следующие команды:

- **Подключиться** - Подключение консоли к удаленному или локальному компьютеру. Подробнее см. в разделе Подключение к компьютеру данного руководства.
- **Переподключиться** - Подключается к текущему компьютеру повторно.
- **Подключаться к локальному компьютеру на старте** - Установите флажок у этой команды для того, чтобы при запуске консоль управления автоматически подключалась к локальному компьютеру.

- **Сбросить политику ContentLock в неопределенное состояние** - Сбрасывает все настройки ContentLock (все правила работы с контентом, кроме тех, которые основаны на типах файлов) в состояние “не задано”.
- **Сбросить политику NetworkLock в неопределенное состояние** - Сбрасывает все настройки NetworkLock в состояние “не задано”.
- **Загрузить настройки сервиса** - Загружает настройки из файла настроек сервиса DeviceLock. Необходимо выбрать файл, созданный путем сохранения настроек сервиса DeviceLock в консоли DeviceLock Service Settings Editor, DeviceLock Management Console или DeviceLock Group Policy Manager.
- **Сохранить настройки сервиса** - Сохраняет текущие настройки сервиса DeviceLock в файл настроек. Позже этот файл может быть загружен в консоли DeviceLock Management Console, DeviceLock Group Policy Manager и/или DeviceLock Service Settings Editor. Также файл настроек может быть отправлен пользователям, чьи компьютеры не подключены к сети и находятся вне досягаемости консолей управления. Во избежание вмешательства в файл настроек следует подписать его, используя для этого Мастер создания подписи. См. также Варианты сохранения файла настроек.
- **Сохранить и подписать настройки сервиса** - Сохраняет текущие настройки сервиса DeviceLock в файл настроек и подписывает его с помощью закрытого ключа последнего используемого сертификата DeviceLock. Эта команда меню недоступна, если в мастере создания подписи ранее не использовался закрытый ключ сертификата DeviceLock. См. также Варианты сохранения файла настроек.
- **Создать MSI-пакет** - Создает MSI-пакет для установки сервиса DeviceLock с настройками, идентичными текущим настройкам сервиса DeviceLock.

  При использовании этой команды вначале выбирается исходный MSI-пакет сервиса DeviceLock. Это может быть один из MSI-пакетов, которые поставляются вместе с DeviceLock (файлы `DeviceLock Service.msi` и `DeviceLock Service x64.msi`).

  Затем требуется указать имя результирующего MSI-пакета, который будет создан на основе исходного MSI пакета и текущих настроек сервиса DeviceLock.

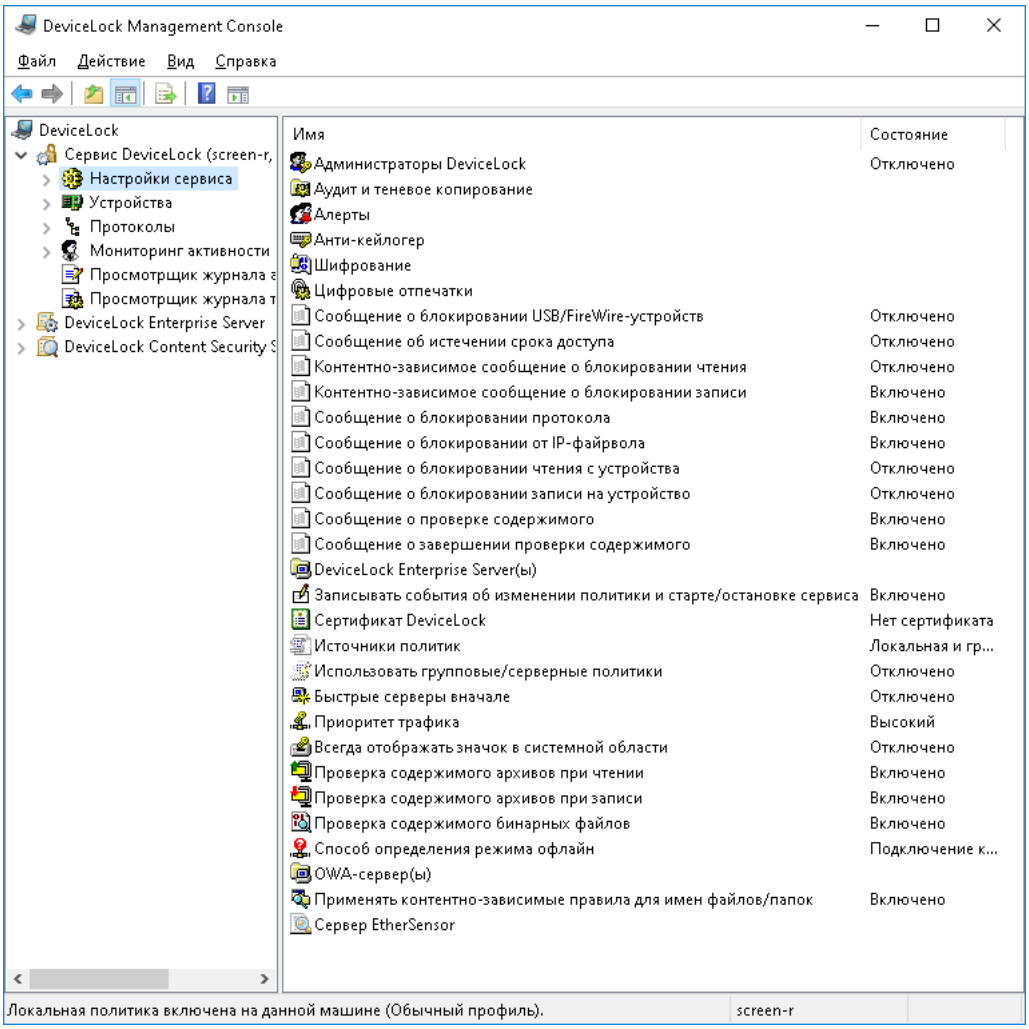
  С помощью такого MSI-пакета сервис DeviceLock с уже определенными политиками безопасности (настройками) можно будет установить на удаленные компьютеры (см. Установка через групповые политики).

  > **Примечание:** При использовании MSI-пакета для развертывания сервиса DeviceLock с помощью групповой политики настройки сервиса, заданные в этом пакете, не применяются на клиентских компьютерах при любом из следующих условий:
  > - На удаленном сервисе DeviceLock выключена безопасность по умолчанию.
  > - В объекте групповой политики, применяемом к клиентским компьютерам, включен параметр DeviceLock **Подавлять локальную политику**.

  Команда контекстного меню **Создать MSI-пакет** недоступна, если Microsoft Windows Installer (версии 1.0 или более поздней) не установлен на локальном компьютере.
- **Мастер создания сертификата** - Запускает программу для создания сертификатов DeviceLock. Подробнее см. в разделе Создание сертификата.
- **Мастер создания подписи** - Запускает программу для авторизации устройств во временном белом списке и подписывания файлов с настройками сервиса DeviceLock. Подробнее см. в разделе Мастер создания подписи.
- **О программе DeviceLock** - Отображает диалоговое окно с информацией о версии и установленных лицензиях на DeviceLock.

Настройки сервиса

Эти параметры позволяют настроить сервис DeviceLock. Для настройки используйте команды контекстного меню, появляющегося по нажатию правой кнопки мыши на каждом параметре.



При настройке сервиса DeviceLock учитывайте следующее:

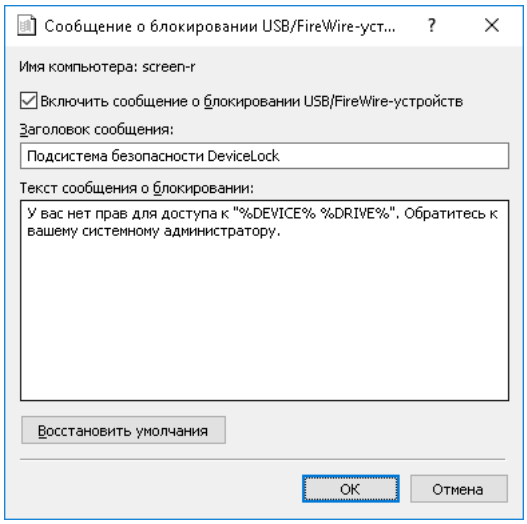
- Настройки сервиса DeviceLock могут неожиданно вернуться в состояние по умолчанию, при этом в консоли DeviceLock Management Console появляется сообщение “Данная машина сконфигурирована для использования настроек групповых политик.” Это сообщение означает, что сервис DeviceLock работает в режиме групповых политик. Локальные настройки перезаписываются настройками из объекта групповой политики.
- Для использования локальных настроек сервиса DeviceLock необходимо отключить параметр Использовать групповые/серверные политики. В противном случае следует задавать настройки сервиса DeviceLock в объекте групповой политики, который действует на данный клиентский компьютер (см. инструкции в разделе DeviceLock Group Policy Manager). Для задания настроек сервиса DeviceLock можно также использовать Политики DeviceLock Enterprise Server.
- Сервис DeviceLock может получать свои настройки от системы киберзащиты Acronis. В строке состояния консоли DeviceLock Management Console при этом отображается сообщение “Политики Acronis Cyber Protect включены на данной машине”, а изменение настроек с помощью консоли DeviceLock Management Console становится невозможным. Для управления сервисом DeviceLock в таком случае необходимо использовать консоль службы киберзащиты Acronis.

Предусмотрены следующие настройки сервиса:

- Сообщение о блокировании USB/FireWire-устройств
- Сообщение об истечении срока доступа
- Контентно-зависимое сообщение о блокировании чтения
- Контентно-зависимое сообщение о блокировании записи
- Сообщение о блокировании протокола
- Сообщение о блокировании от IP-файрвола
- Сообщение о блокировании чтения с устройства
- Сообщение о блокировании записи на устройство
- Сообщение о проверке содержимого
- Сообщение о завершении проверки содержимого
- DeviceLock Enterprise Server(ы)
- Записывать события об изменении политики и старте/остановке сервиса
- Сертификат DeviceLock
- Источники политик
- Использовать групповые/серверные политики
- Быстрые серверы вначале
- Приоритет трафика
- Всегда отображать значок в системной области
- Проверка содержимого архивов при чтении
- Проверка содержимого архивов при записи
- Проверка содержимого бинарных файлов
- Способ определения режима офлайн
- OWA-сервер(ы)
- Применять контентно-зависимые правила для имен файлов/папок
- Сервер EtherSensor
- Администраторы DeviceLock
- Аудит и теневое копирование
- Алерты
- Анти-кейлогер
- Шифрование
- Цифровые отпечатки

Сообщение о блокировании USB/FireWire-устройств

Этот параметр позволяет задать сообщение для отображения пользователю при подключении USB или FireWire-устройств, запрещенных на уровне интерфейса (**USB** или **FireWire**) или на уровне типа (**Съемные устройства**, **Оптический привод** и т. п.).



Чтобы разрешить отображение этого пользовательского сообщения, установите флажок **Включить сообщение о блокировании USB/FireWire-устройств**.

Для данного параметра предусмотрены следующие настройки:

- **Заголовок сообщения** - Текст, который будет отображаться в заголовке.
- **Текст сообщения о блокировании** - Основной текст сообщения.

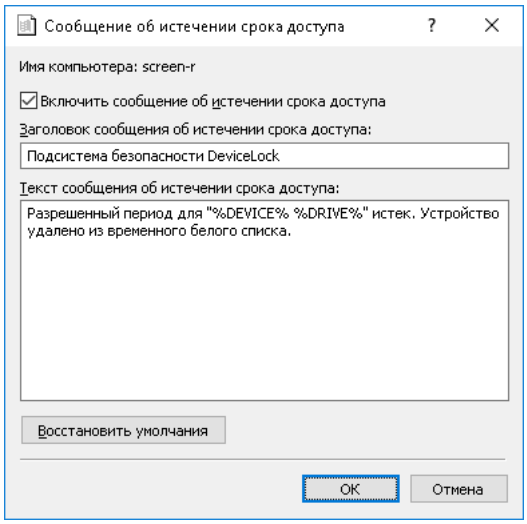
В заголовке и тексте сообщения можно использовать макросы, делающие сообщение более информативным для пользователя:

- `%TYPE%` - Имя порта (например, USB-порт, FireWire-порт), к которому подключено заблокированное устройство.
- `%DEVICE%` - Имя устройства (например, USB-накопитель), полученное от операционной системы.
- `%DRIVE%` - Буква, назначенная устройству в операционной системе (например, F:). Если буква не назначена, макрос вставит в текст пустую строку.

Примечание: При использовании терминального сервера сообщение может быть показано всем зарегистрированным пользователям сервера, которым запрещен доступ к портам USB или FireWire, если кто-нибудь из них попытается использовать такой порт.

Сообщение об истечении срока доступа

Этот параметр позволяет задать сообщение для отображения пользователю по истечении разрешенного периода использования устройств, авторизованных через функцию временного белого списка (см. раздел Временный белый список).



Чтобы разрешить отображение этого пользовательского сообщения, установите флажок **Включить сообщение об истечении срока доступа**.

Для данного параметра предусмотрены следующие настройки:

- **Заголовок сообщения об истечении срока доступа** - Текст, который будет отображаться в заголовке.
- **Текст сообщения об истечении срока доступа** - Основной текст сообщения.

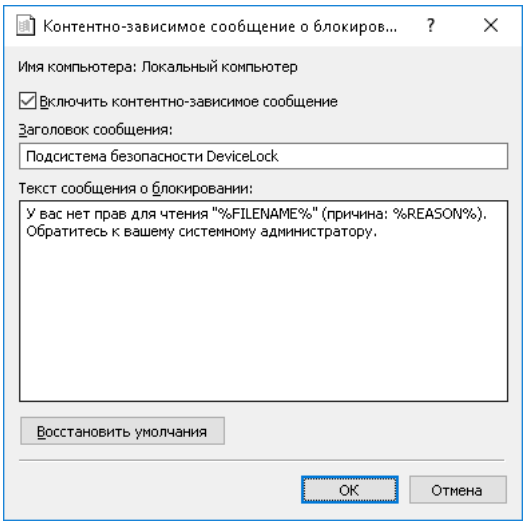
В заголовке и тексте сообщения можно использовать макросы, делающие сообщение более информативным для пользователя:

- `%DEVICE%` - Имя устройства (например, USB-накопитель), полученное от операционной системы.
- `%DRIVE%` - Буква, назначенная устройству в операционной системе (например, F:). Если буква не назначена, макрос вставит в текст пустую строку.

Контентно-зависимое сообщение о блокировании чтения

Этот параметр позволяет задать всплывающее сообщение о блокировании чтения, которое будет отображаться пользователям при попытке чтения запрещенного содержимого файлов. Данное сообщение появляется в области уведомлений панели задач на клиентских компьютерах. По умолчанию DeviceLock не выводит сообщение о блокировании чтения.

Чтобы включить или отключить показ сообщения о блокировании чтения, щелкните правой кнопкой мыши элемент **Контентно-зависимое сообщение о блокировании чтения** и выберите команду **Свойства** или дважды щелкните элемент **Контентно-зависимое сообщение о блокировании чтения**.



В диалоговом окне **Контентно-зависимое сообщение о блокировании чтения** выполните следующее:

- **Включить контентно-зависимое сообщение** - Включить или отключить сообщение о блокировании чтения.

  Установите флажок **Включить контентно-зависимое сообщение**, чтобы разрешить отображение данного сообщения.

  Снимите флажок **Включить контентно-зависимое сообщение**, чтобы запретить отображение данного сообщения.

- **Заголовок сообщения** - Задать текст для заголовка всплывающего сообщения.

  Заголовок по умолчанию: “Подсистема безопасности DeviceLock”

- **Текст сообщения о блокировании** - Задать текст всплывающего сообщения.

  Текст сообщения по умолчанию: “У вас нет прав для чтения "`%FILENAME%`" (причина: `%REASON%`). Обратитесь к вашему системному администратору.”

  В этом сообщении `%FILENAME%` представляет путь и имя файла, `%REASON%` описывает причину блокирования доступа к файлу.

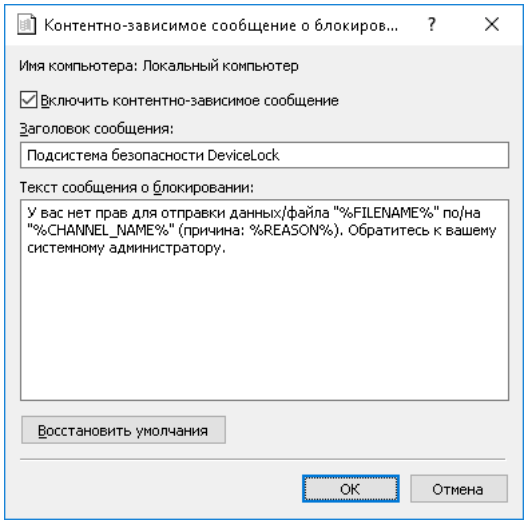
- **Восстановить умолчания** - Восстановить настройки по умолчанию.

Подробное описание функциональности контентно-зависимых правил см. в разделе Контентно-зависимые правила (обычный профиль).

Контентно-зависимое сообщение о блокировании записи

Этот параметр позволяет задать всплывающее сообщение о блокировании записи, которое будет отображаться пользователям при попытке записи запрещенного содержимого файлов или при передаче запрещенных данных. Данное сообщение появляется в области уведомлений панели задач на клиентских компьютерах. По умолчанию DeviceLock выводит сообщение о блокировании записи.

Чтобы включить или отключить показ сообщения о блокировании записи, щелкните правой кнопкой мыши элемент **Контентно-зависимое сообщение о блокировании записи** и выберите команду **Свойства** или дважды щелкните элемент **Контентно-зависимое сообщение о блокировании записи**.



В диалоговом окне **Контентно-зависимое сообщение о блокировании записи** выполните следующее:

- **Включить контентно-зависимое сообщение** - Включить или отключить сообщение о блокировании записи.

  Установите флажок **Включить контентно-зависимое сообщение**, чтобы разрешить отображение данного сообщения.

  Снимите флажок **Включить контентно-зависимое сообщение**, чтобы запретить отображение данного сообщения.

- **Заголовок сообщения** - Задать текст для заголовка всплывающего сообщения.

  Заголовок по умолчанию: “Подсистема безопасности DeviceLock”

- **Текст сообщения о блокировании** - Задать текст всплывающего сообщения.

  Текст сообщения по умолчанию: “У вас нет прав для отправки данных/файла "`%FILENAME%`" по/на "`%CHANNEL_NAME%`" (причина: `%REASON%`). Обратитесь к вашему системному администратору.”

  В этом сообщении `%FILENAME%` представляет путь и имя файла, `%CHANNEL_NAME%` указывает канал передачи данных, `%REASON%` описывает причину блокирования доступа к файлу.

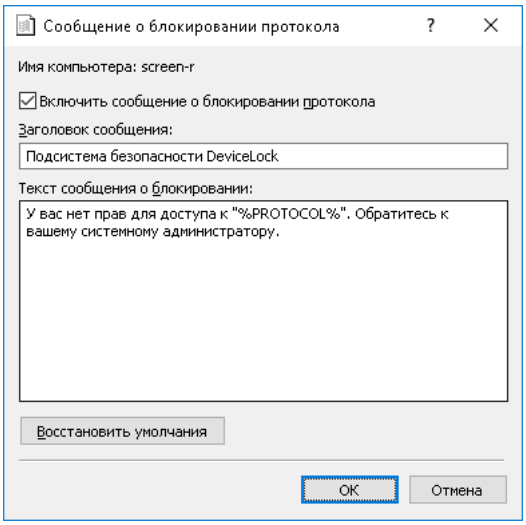
- **Восстановить умолчания** - Восстановить настройки по умолчанию.

Подробное описание функциональности контентно-зависимых правил см. в разделе Контентно-зависимые правила (обычный профиль).

Сообщение о блокировании протокола

Этот параметр позволяет задать всплывающее сообщение о блокировании доступа к сетевому протоколу, которое будет отображаться пользователям при попытке использовать запрещенный сетевой протокол. Данное сообщение появляется в области уведомлений панели задач на клиентских компьютерах.

Чтобы включить или отключить показ сообщения о блокировании доступа к сетевому протоколу, щелкните правой кнопкой мыши элемент **Сообщение о блокировании протокола** и выберите команду **Свойства** или дважды щелкните элемент **Сообщение о блокировании протокола**.



В диалоговом окне **Сообщение о блокировании протокола** выполните следующее:

- **Включить сообщение о блокировании протокола** - Включить или отключить сообщение о блокировании сетевого протокола.

  Установите флажок **Включить сообщение о блокировании протокола**, чтобы разрешить отображение данного сообщения.

  Снимите флажок **Включить сообщение о блокировании протокола**, чтобы запретить отображение данного сообщения.

- **Заголовок сообщения** - Задать текст для заголовка всплывающего сообщения.

  Заголовок по умолчанию: “Подсистема безопасности DeviceLock”

- **Текст сообщения о блокировании** - Задать текст всплывающего сообщения.

  Текст сообщения по умолчанию: “У вас нет прав для доступа к "`%PROTOCOL%`". Обратитесь к вашему системному администратору.”

- **Восстановить умолчания** - Восстановить настройки по умолчанию.

В заголовке и тексте сообщения можно использовать макросы, делающие сообщение более информативным для пользователя:

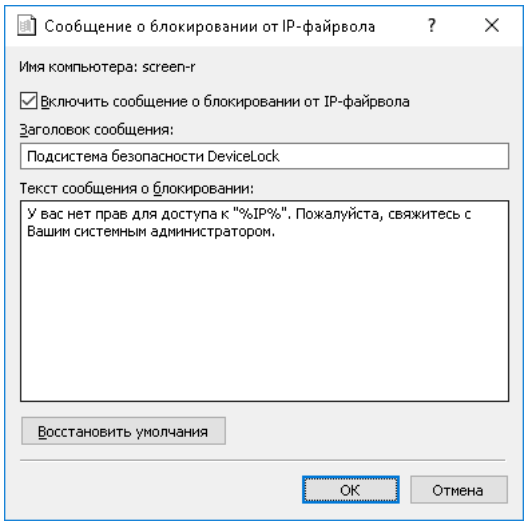
- `%PROTOCOL%` - Имя заблокированного сетевого протокола.
- `%IP%` - IP-адрес и/или имя ресурса, доступ к которому заблокирован. Если установить имя ресурса невозможно, отображается только IP-адрес. Если невозможно установить IP-адрес, то отображается только имя ресурса.

Подробное описание функциональности контроля протоколов см. в разделе Протоколы (обычный профиль).

Сообщение о блокировании от IP-файрвола

Этот параметр позволяет задать сообщение о блокировании доступа Базовым IP-файрволом, которое будет отображаться пользователям при попытке подключения к запрещенному для них узлу.

Чтобы включить или отключить показ данного сообщения, щелкните правой кнопкой мыши элемент **Сообщение о блокировании от IP-файрвола** и выберите команду **Свойства** или дважды щелкните элемент **Сообщение о блокировании от IP-файрвола**.



В диалоговом окне **Сообщение о блокировании от IP-файрвола** выполните следующее:

- **Включить сообщение о блокировании от IP-файрвола** - Включить или отключить сообщение о блокировании Базовым IP-файрволом доступа к IP-адресу.

  Установите флажок **Включить сообщение о блокировании от IP-файрвола**, чтобы разрешить отображение данного сообщения.

  Снимите флажок **Включить сообщение о блокировании от IP-файрвола**, чтобы запретить отображение данного сообщения.

- **Заголовок сообщения** - Задать текст для заголовка окна сообщения.

  По умолчанию DeviceLock отображает окно сообщения со следующим заголовком: **Подсистема безопасности DeviceLock**

- **Текст сообщения о блокировании** - Задать текст, отображаемый в окне сообщения.

  По умолчанию используется следующий текст сообщения: “У вас нет прав для доступа к "`%IP%`". Пожалуйста, свяжитесь с Вашим системным администратором.”

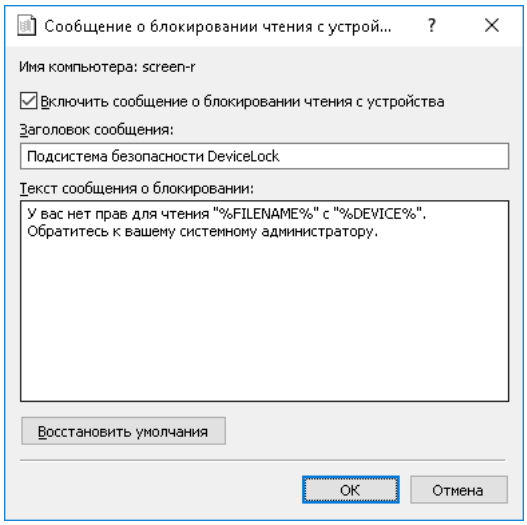
  На месте макроса `%IP%` в сообщении отображается IP-адрес и/или имя узла, доступ к которому заблокирован. Если установить имя узла невозможно, отображается только IP-адрес. Если невозможно установить IP-адрес, то отображается только имя узла.

- **Восстановить умолчания** - Восстановить настройки по умолчанию.

Подробное описание функциональности IP-файрвола см. в разделе Базовый IP-файрвол.

Сообщение о блокировании чтения с устройства

Этот параметр задает сообщение, которое будет показано пользователю при запрете попытки чтения данных с устройств следующих типов: Гибкий диск, Жесткий диск, Оптический привод, Съемные устройства, Ленточные накопители, MTP, iPhone-устройства, Palm, Windows Mobile, TC-устройства (при запрете на Чтение с подключенного диска, Буфер обмена входящий текст, Буфер обмена входящие изображения, Буфер обмена входящие аудио данные, Буфер обмена входящие файлы или Буфер обмена входящие неизвестные данные).



Чтобы разрешить отображение этого пользовательского сообщения, установите флажок **Включить сообщение о блокировании чтения с устройства**.

Примечание:

- Это сообщение будет также показано пользователю при запрете попытки чтения или записи на устройства следующих типов: Blackberry-устройства, Bluetooth, FireWire-порт, ИК-порт, Параллельный порт, Последовательный порт, TC-устройства (при запрете на Доступ к USB-устройствам или Доступ к последовательному порту), USB-порт, WiFi.
- Сообщение отображается пользователю в момент попытки совершения запрещенной ему операции.
- Когда доступ к устройствам WiFi или Bluetooth запрещен, данное сообщение отображается только один раз. Следующий показ сообщения возможен только при изменении настроек для этих устройств.

Для данного параметра предусмотрены следующие настройки:

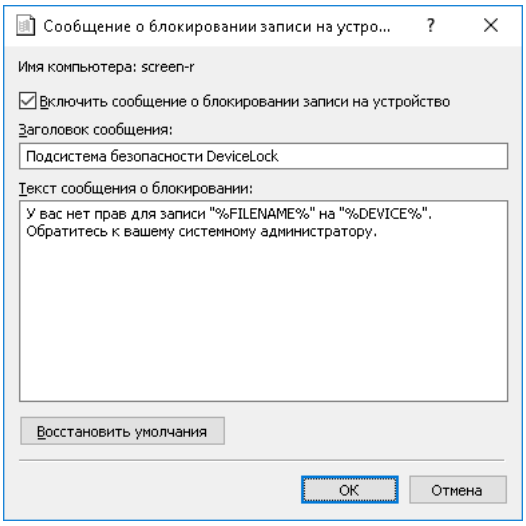
- **Заголовок сообщения** - Текст, который будет отображаться в заголовке.
- **Текст сообщения о блокировании** - Основной текст сообщения. В этом тексте также можно использовать макросы, описанные выше.

В заголовке и тексте сообщения можно использовать макросы, делающие сообщение более информативным для пользователя:

- `%FILENAME%` - Имя файла для чтения.
- `%DEVICE%` - Имя устройства (например, USB-накопитель), полученное от операционной системы.

Сообщение о блокировании записи на устройство

Этот параметр задает сообщение, которое будет показано пользователю при запрете попытки записи данных на устройства следующих типов: Гибкий диск, Жесткий диск, Оптический привод, Съемные устройства, Ленточные накопители, MTP, iPhone-устройства, Palm, Windows Mobile, Принтер, Буфер обмена (при запрете на Копирование текста, Копирование файла, Копирование изображения, Копирование аудио данных, Копирование экрана или Копирование неидентифицированного содержимого), TC-устройства (при запрете на Запись на подключенный диск, Буфер обмена исходящий текст, Буфер обмена исходящие изображения, Буфер обмена исходящие аудио данные, Буфер обмена исходящие файлы или Буфер обмена исходящие неизвестные данные).



Чтобы разрешить отображение этого пользовательского сообщения, установите флажок **Включить сообщение о блокировании записи на устройство**.

Примечание:

- Сообщение отображается пользователю в момент попытки совершения запрещенной ему операции.
- Это сообщение не будет показано пользователю при запрете попытки записи на устройства следующих типов: Blackberry-устройства, Bluetooth, FireWire-порт, ИК-порт, Параллельный порт, Последовательный порт, TC-устройства (при запрете на Доступ к USB-устройствам или Доступ к последовательному порту), USB-порт, WiFi. В этом случае показывается сообщение о блокировании чтения с устройства.

Для данного параметра предусмотрены следующие настройки:

- **Заголовок сообщения** - Текст, который будет отображаться в заголовке.
- **Текст сообщения о блокировании** - Основной текст сообщения.

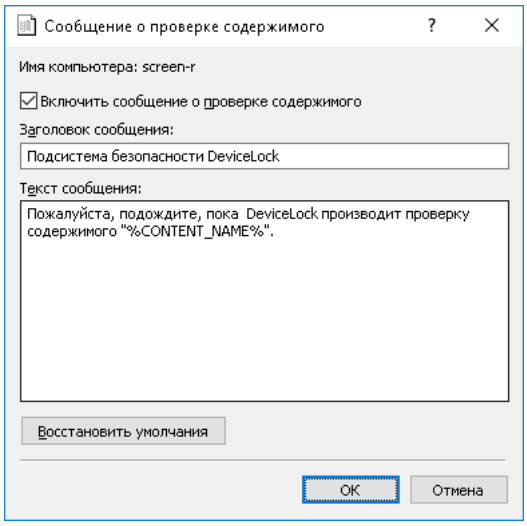
В заголовке и тексте сообщения можно использовать макросы, делающие сообщение более информативным для пользователя:

- `%FILENAME%` - Имя файла для записи.
- `%DEVICE%` - Имя устройства (например, USB-накопитель), полученное от операционной системы.

Сообщение о проверке содержимого

Проверка содержимого файлов, копируемых на устройства или передаваемых по сети, может занимать длительное время. Данный параметр позволяет задать сообщение о проверке содержимого, которое будет отображаться пользователям во время проверки. Это сообщение появляется через 20 секунд после начала проверки.

Чтобы включить или отключить показ данного сообщения, щелкните правой кнопкой мыши элемент **Сообщение о проверке содержимого** и выберите команду **Свойства** или дважды щелкните элемент **Сообщение о проверке содержимого**.



В диалоговом окне **Сообщение о проверке содержимого** выполните следующее:

- **Включить сообщение о проверке содержимого** - Включить или отключить сообщение о проверке содержимого.

  Установите флажок **Включить сообщение о проверке содержимого**, чтобы разрешить отображение данного сообщения.

  Снимите флажок **Включить сообщение о проверке содержимого**, чтобы запретить отображение данного сообщения.

- **Заголовок сообщения** - Задать текст для заголовка окна сообщения.

  Заголовок по умолчанию: “Подсистема безопасности DeviceLock”

- **Текст сообщения** - Задать текст, отображаемый в окне сообщения.

  Текст сообщения по умолчанию: “Пожалуйста, подождите, пока DeviceLock производит проверку содержимого "`%CONTENT_NAME%`"”

  Вместо макроса `%CONTENT_NAME%` в сообщение отображается имя файла (при проверке файла, копируемого на устройство) или имя сетевого протокола (при проверке данных, передаваемых по этому протоколу).

- **Восстановить умолчания** - Восстановить настройки по умолчанию.

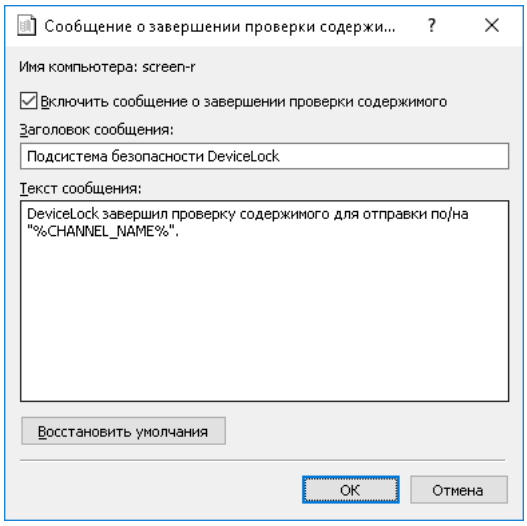
Подробное описание функциональности контентно-зависимых правил см. в разделе Контентно-зависимые правила (обычный профиль).

Сообщение о завершении проверки содержимого

Этот параметр позволяет задать сообщение о завершении проверки содержимого, которое будет отображаться пользователям после завершения проверки записанного на устройство контента в соответствии с заданными контентно-зависимыми правилами. Сообщение отображается при записи контента на съемные устройства или на подключенные диски категории **ТС-устройства**.

Примечание: После показа этого сообщения пользователь может безопасно извлечь устройство при помощи приложения безопасного извлечения. Однако в некоторых случаях нельзя гарантировать безопасное извлечение устройства немедленно после показа этого сообщения.

Чтобы включить или отключить показ данного сообщения, щелкните правой кнопкой мыши элемент **Сообщение о завершении проверки содержимого** и выберите команду **Свойства** или дважды щелкните элемент **Сообщение о завершении проверки содержимого**.



В диалоговом окне **Сообщение о завершении проверки содержимого** выполните следующее:

- **Включить сообщение о завершении проверки содержимого** - Включить или отключить сообщение о завершении проверки содержимого.

  Установите флажок **Включить сообщение о завершении проверки содержимого**, чтобы разрешить отображение данного сообщения.

  Снимите флажок **Включить сообщение о завершении проверки содержимого**, чтобы запретить отображение данного сообщения.

- **Заголовок сообщения** - Задать текст для заголовка окна сообщения.

  Заголовок по умолчанию: “Подсистема безопасности DeviceLock”

- **Текст сообщения** - Задать текст, отображаемый в окне сообщения.

  Текст сообщения по умолчанию: “DeviceLock завершил проверку содержимого для отправки по/на "`%CHANNEL_NAME%`"”

  В этом сообщении `%CHANNEL_NAME%` указывает имя канала передачи данных.

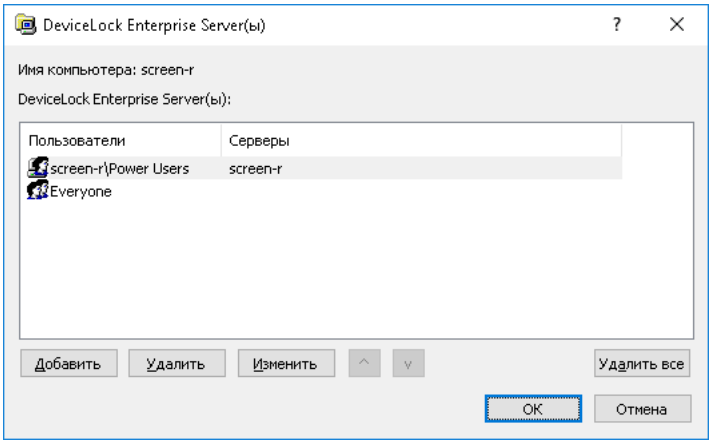
- **Восстановить умолчания** - Восстановить настройки по умолчанию.

Подробное описание функциональности контентно-зависимых правил см. в разделе Контентно-зависимые правила (обычный профиль).

DeviceLock Enterprise Server(ы)

Чтобы позволить сервису DeviceLock отправлять данные своих журналов на сервер DeviceLock Enterprise Server, укажите имя или IP-адрес этого сервера. Для балансирования нагрузки можно распределить данные разных пользователей по различным серверам, задавая серверы для каждого пользователя или для группы пользователей. Данные, относящиеся к указанному пользователю или группе, отправляются на заданный сервер. Если раздельный сбор журналов по пользователям не требуется, следует задать сервер для группы **Все**, что позволит сервису DeviceLock отправлять на этот сервер данные, относящиеся к любым пользователям.

Дважды щелкните **DeviceLock Enterprise Server(ы)** на панели сведений, чтобы открыть диалоговое окно для настройки списка серверов.



В диалоговом окне **DeviceLock Enterprise Server(ы)** можно просмотреть или изменить список серверов:

- **Пользователи** - Отображается список пользователей и групп, для которых заданы серверы. Первоначально список содержит только группу **Все**. Используйте кнопку **Добавить** или **Удалить**, чтобы добавить или удалить пользователя или группу из списка. По щелчку кнопки **Добавить** открывается стандартное диалоговое окно для выбора пользователей и групп. Чтобы удалить всех пользователей и группы, кроме группы **Все**, нажмите кнопку **Удалить все**. Удалить группу **Все** невозможно.
- **Серверы** - Для каждого пользователя или группы указывается один или несколько компьютеров, на которых установлен DeviceLock Enterprise Server. Выберите пользователя или группу и нажмите кнопку **Изменить**, чтобы внести изменения в поле **Серверы** для этого пользователя или группы. Можно также нажать F2 или дважды щелкнуть в поле **Серверы**.

  Сервис DeviceLock отправляет данные журналов, относящиеся к определенному пользователю или группе пользователей, на сервер, указанный в поле **Серверы** для этого пользователя или группы. Если указать сервер для группы **Все**, сервис DeviceLock будет отправлять на этот сервер данные журналов, относящиеся к любым пользователям.

  Можно указать несколько серверов, используя точку с запятой (;) для разделения имен в поле **Серверы**. Сервис DeviceLock выбирает один из этих серверов, доступный в сети. Выбор сервера также зависит от параметра Быстрые серверы вначале.

  Если пользователю назначено несколько серверов по причине его участия в нескольких группах, каждой из которых назначен некоторый сервер, то можно установить приоритет серверов с помощью кнопок со стрелками вверх и вниз для перемещения этих групп вверх или вниз по списку. Сервис DeviceLock сначала попытается использовать серверы, которые находятся выше в списке. Серверы, назначенные только группе **Все**, всегда выбираются последними: эта группа стоит внизу списка и ее невозможно переместить.

Убедитесь в том, что DeviceLock Enterprise Server правильно установлен и настроен, иначе данные не будут собираться и храниться централизованно. Инструкции по установке сервера можно найти в разделе Установка DeviceLock Enterprise Server данного руководства.

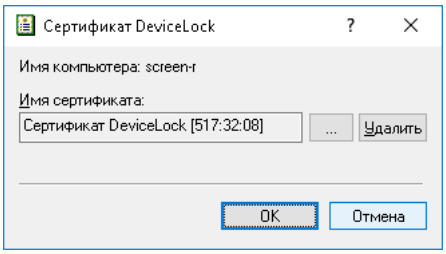
Записывать события об изменении политики и старте/остановке сервиса

Данный параметр позволяет включить протоколирование изменений в настройках сервиса DeviceLock и фиксацию времени старта и остановки сервиса. Протоколируются изменения разрешений, правил аудита, белых списков и всех остальных настроек.

Для включения такого протоколирования включите параметр **Записывать события об изменении политики и старте/остановке сервиса**.

Сертификат DeviceLock

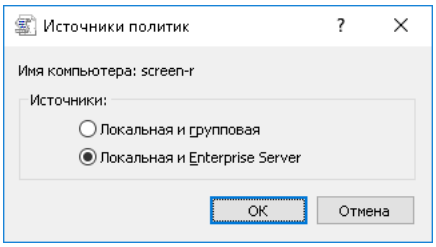
Данный параметр служит для установки и удаления открытого ключа сертификата DeviceLock.



Для установки ключа нажмите кнопку ... рядом с полем **Имя сертификата** и укажите файл, содержащий открытый ключ сертификата. Для удаления ключа используйте кнопку **Удалить**. Подробнее о сертификатах DeviceLock см. в разделе Сертификаты DeviceLock.

Источники политик

Данный параметр используется совместно с параметром Использовать групповые/серверные политики для определения источника, из которого сервис DeviceLock получает свои настройки.



Возможные значения параметра:

- **Локальная и групповая** - Сервис DeviceLock получает настройки из объекта групповой политики либо использует локально заданные настройки в зависимости от параметра Использовать групповые/серверные политики.
- **Локальная и Enterprise Server** - Сервис DeviceLock получает настройки из объекта политики сервера DeviceLock Enterprise Server либо использует локально заданные настройки в зависимости от параметра Использовать групповые/серверные политики.

По умолчанию для выбора источника групповых/серверных политик используется неявно заданное значение **Любой**, при котором будет применена первая полученная политика - групповая либо Enterprise Server, после чего будет автоматически установлен выбор источника политики - **Локальная и групповая** либо **Локальная и Enterprise Server** соответственно.

Внимание: Сервис DeviceLock может получать свои настройки от системы киберзащиты Acronis. В этом случае параметр **Источники политик** не действует, а для управления сервисом DeviceLock необходимо использовать консоль службы киберзащиты Acronis.

Использовать групповые/серверные политики

Если этот параметр находится в состоянии **Отключено**, то для данного сервиса DeviceLock действуют локальные настройки (режим локальной политики). Если этот параметр находится в состоянии **Включено**, то действующие настройки определяются групповой политикой службы доменов Active Directory (Group Policy) или серверной политикой DeviceLock Enterprise Server, в зависимости от параметра Источники политик.

Если компьютер настроен для работы с групповой политикой, параметр **Использовать групповые/серверные политики** позволяет выбрать режим групповой или локальной политики для сервиса DeviceLock. Включите этот параметр для выбора групповой политики. Настройки, заданные в консоли DeviceLock Management Console или DeviceLock Enterprise Manager, будут заменяться настройками групповой политики. Отключите этот параметр для выбора локальной политики. Настройки, заданные в консоли DeviceLock Management Console или DeviceLock Enterprise Manager, будут иметь приоритет над настройками групповой политики.

Если компьютер настроен для работы с политикой сервера (см. Политики DeviceLock Enterprise Server), параметр **Использовать групповые/серверные политики** позволяет выбрать режим серверной или локальной политики для сервиса DeviceLock. Включите этот параметр для выбора серверной политики. Настройки, заданные в консоли DeviceLock Management Console или DeviceLock Enterprise Manager, будут заменяться настройками политики сервера. Отключите этот параметр для выбора локальной политики. Настройки, заданные в консоли DeviceLock Management Console или DeviceLock Enterprise Manager, будут иметь приоритет над настройками политики сервера DeviceLock Enterprise Server.

Если компьютер не настроен для работы с групповой или серверной политикой, параметр **Использовать групповые/серверные политики** отключен и недоступен для изменения.

Если параметр **Использовать групповые/серверные политики** включен и недоступен для изменения, это означает, что групповая или серверная политика всегда имеет приоритет, т.к. в DeviceLock Group Policy Manager или в политике сервера DeviceLock Enterprise Server включен параметр **Подавлять локальную политику**. Описание этого параметра приводится в разделе Использование DeviceLock Group Policy Manager.

Внимание: Сервис DeviceLock может получать свои настройки от системы киберзащиты Acronis. В этом случае параметр **Использовать групповые/серверные политики** не действует, а для управления сервисом DeviceLock необходимо использовать консоль службы киберзащиты Acronis.

Рекомендации

При включенном параметре **Использовать групповые/серверные политики** любые настройки, заданные в консоли DeviceLock Management Console, через некоторое время перезаписываются настройками, полученными извне. В зависимости от параметра Источники политик настройки могут поступить из объекта групповой политики (GPO) или от сервера DeviceLock Enterprise Server. Одновременное использование локальных и внешних настроек невозможно.

Таким образом, групповая/серверная политика и локальная политика не могут одновременно применяться к одному и тому же компьютеру. Если же требуется, чтобы один из компьютеров использовал локальные настройки, в то время как другие компьютеры получали бы свои настройки из GPO или от сервера, следует отключить параметр **Использовать групповые/серверные политики** для этого конкретного компьютера. В результате компьютер перестанет получать настройки из внешнего источника, и будет применена локальная политика.

Если к компьютеру применен объект групповой политики или объект политики сервера, консоль может не позволить отключить параметр **Использовать групповые/серверные политики**. Обычно это вызвано тем, что в объекте политики включен параметр **Подавлять локальную политику**. Отключите этот параметр в объекте политики или удалите компьютер из области действия GPO или из объекта политики сервера. В случае GPO можно переместить компьютер в другое подразделение домена Active Directory, где не данный GPO не действует. В случае объекта политики сервера используйте инструкции, приведенные в разделе Изменение объекта политики на клиентском компьютере.

Быстрые серверы вначале

Сервис DeviceLock может выбирать из списка наиболее быстрый из доступных серверов.

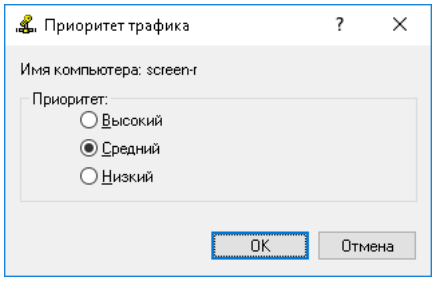
Если параметр **Быстрые серверы вначале** включен, то все сервера, указанные в параметре **DeviceLock Enterprise Server(ы)**, разделяются на три группы в зависимости от их сетевой скорости. Вначале предпочтение отдается одному из доступных серверов из самой быстрой группы. Если все сервера из быстрой группы недоступны, сервис DeviceLock пытается выбрать сервер из следующей группы и так далее.

Если этот параметр отключен, то сервис DeviceLock выбирает сервер из списка случайным образом.

Данный параметр имеет силу только если в параметре **DeviceLock Enterprise Server(ы)** задано больше одного сервера.

Приоритет трафика

Данный параметр позволяет ограничить использование пропускной способности сети при передаче журналов аудита и теневого копирования от сервиса DeviceLock на сервер DeviceLock Enterprise Server.



В диалоговом окне, появляющемся по двойному щелчку параметра **Приоритет трафика**, можно выбрать один из следующих вариантов приоритета с целью ограничить использование пропускной способности сети для передачи журналов на сервер:

- **Высокий** - Использовать всю доступную пропускную способность сети.
- **Средний** - Использовать не более 50% пропускной способности сети.
- **Низкий** - Использовать не более 20% пропускной способности сети.

Внимание: Для управления приоритетом трафика необходимо, чтобы планировщик пакетов QoS (QoS Packet Scheduler) был включен у сетевого подключения компьютера, на котором работает сервис DeviceLock. В противном случае задать приоритет трафика невозможно, и для передачи журналов используется вся доступная пропускная способность сети.

Всегда отображать значок в системной области

Данный параметр позволяет отобразить или скрыть значок DeviceLock в области уведомлений (системном трее) на панели задач компьютера, на котором работает сервис DeviceLock. Когда этот параметр включен, в области уведомлений появляется значок DeviceLock . Отключение этого параметра скрывает значок DeviceLock.

Внешний вид значка зависит от текущего режима работы DeviceLock:

- - Оперативный режим (онлайн). Используется обычный профиль.
- - Автономный режим (офлайн). Используется офлайн-профиль.
- - Определение текущего состояния подключения (определение статуса). Используется профиль, соответствующий предыдущему состоянию подключения.

Если навести указатель мыши на значок DeviceLock, появятся следующие сведения:

- Версия и номер сборки DeviceLock.
- Текущий режим работы DeviceLock (онлайн, офлайн, либо определение статуса) в соответствии с внешним видом значка DeviceLock.

По щелчку на значке DeviceLock появляется последнее уведомление DeviceLock, полученное на данном компьютере.

Если значок DeviceLock щелкнуть правой кнопкой мыши, появятся следующие команды:

- **Показать историю сообщений** - Отобразить все уведомления DeviceLock, появлявшиеся с момента последнего запуска сервиса DeviceLock.
- **Обновить текущее состояние** - Определить текущее состояние соединения и соответственно выбрать режим работы.
- **Апплет DeviceLock** - Открыть приложение DeviceLock, позволяющее:
  - Получить временный доступ к устройству (см. Получение временного доступа).
  - Загрузить подписанный файл с новыми настройками (см. Загрузка подписанного файла настроек на Windows).

Чтобы отобразить или скрыть значок DeviceLock, щелкните правой кнопкой мыши параметр **Всегда отображать значок в системной области** и выберите команду **Включить** или **Отключить**, либо дважды щелкните этот параметр.

Проверка содержимого архивов при чтении

Данный параметр используется, чтобы разрешить или запретить контентную проверку файлов, содержащихся в архивах, при попытках пользователя читать архивный файл. Подробнее см. в описании функции Проверка файлов внутри архивов. Чтобы разрешить или запретить контентную проверку файлов при чтении архивных файлов, щелкните правой кнопкой мыши элемент **Проверка содержимого архивов при чтении** и выберите команду **Включить** или **Выключить**, или дважды щелкните этот элемент.

Примечание:

- Если этот параметр включен, может произойти сбой при проверке файла (архива, документа Microsoft Office или файла PDF), защищенного паролем, поскольку из такого файла не удается извлечь контент для проверки. В этом случае DeviceLock блокирует передачу файла из-за сбоя проверки контента.
- Если этот параметр отключен, проверка документов, встроенных в файлы сохраненных писем (EML), Adobe Portable Document Format (PDF), Rich Text Format (RTF), файлы AutoCAD (.dwg, .dxf) и в документы Microsoft Office (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx), также не будет выполняться.

Проверка содержимого архивов при записи

Данный параметр используется, чтобы разрешить или запретить контентную проверку файлов, содержащихся в архивах, при попытках пользователя записать или передать архивный файл. Подробнее см. в описании функции Проверка файлов внутри архивов. Чтобы разрешить или запретить контентную проверку файлов при записи архивных файлов, щелкните правой кнопкой мыши элемент **Проверка содержимого архивов при записи** и выберите команду **Включить** или **Выключить**, или дважды щелкните этот элемент.

Примечание:

- Если этот параметр включен, может произойти сбой при проверке файла (архива, документа Microsoft Office или файла PDF), защищенного паролем, поскольку из такого файла не удается извлечь контент для проверки. В этом случае DeviceLock блокирует передачу файла из-за сбоя проверки контента.
- Если этот параметр отключен, проверка документов, встроенных в файлы сохраненных писем (EML), Adobe Portable Document Format (PDF), Rich Text Format (RTF), файлы AutoCAD (.dwg, .dxf) и в документы Microsoft Office (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx), также не будет выполняться.

Проверка содержимого бинарных файлов

Параметр **Проверка содержимого бинарных файлов** позволяет проверять текстовый контент, содержащийся в произвольных двоичных файлах. Когда этот параметр отключен, DeviceLock выполняет контентный анализ на основе ключевых слов и текстовых шаблонов только для текста в кодировке Unicode в определенных типах файлов (список см. в пункте Поддержка множества типов файлов и данных раздела Модули ContentLock и NetworkLock).

Когда этот параметр включен, DeviceLock выполняет контентный анализ на основе ключевых слов и текстовых шаблонов для текста, содержащегося в любых двоичных файлах, независимо от кодировки текста (Unicode или не-Unicode). В этом случае проверка контента может занять значительно больше времени.

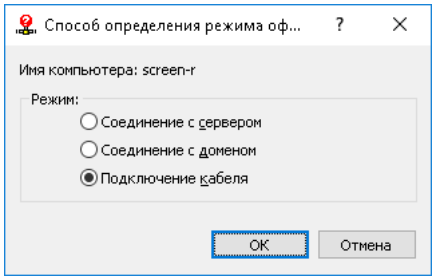
Примечание: Данный параметр влияет на контентно-зависимые правила, в которых используются группы ключевых слов, группы шаблонов и/или содержащие их составные контентные группы. Подробнее о контентно-зависимых правилах см. в разделе Контентно-зависимые правила (обычный профиль).

Чтобы включить или отключить этот параметр, дважды щелкните элемент **Проверка содержимого бинарных файлов** в списке **Настройки сервиса**, или щелкните этот элемент правой кнопкой мыши и выберите команду **Включить** или **Выключить**.

Способ определения режима офлайн

Этот параметр используется, чтобы настроить конфигурацию для автономного режима. Можно указать сетевые характеристики, которые DeviceLock будет использовать для проверки текущего состояния сетевого подключения (подключен или отключен). По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру.

Чтобы настроить конфигурацию для автономного режима, щелкните правой кнопкой мыши элемент **Способ определения режима офлайн** и выберите команду **Свойства** или дважды щелкните этот элемент.



Можно выбрать один из следующих вариантов:

- **Соединение с сервером** - Состояние подключения определяется тем, можно ли передать журналы сервиса DeviceLock с клиентского компьютера на сервер DeviceLock Enterprise Server.

  Считается, что компьютер работает в оперативном режиме, если сервер может получать журналы DeviceLock хотя бы для одного пользователя, использующего этот компьютер в данный момент. Сервер определяется параметром DeviceLock Enterprise Server(ы) в настройках сервиса DeviceLock.

  Компьютер считается работающим в автономном режиме, если сервер не в состоянии получить журналы DeviceLock ни для одного из пользователей, которые в данный момент используют этот компьютер. Это может произойти из-за того, что сервису DeviceLock не удается пройти проверку подлинности ни на одном из назначенных серверов DeviceLock Enterprise Server, или все назначенные серверы недоступны.

- **Соединение с доменом** - Состояние подключения определяется наличием соединения с контроллером домена Active Directory, в который входит данный клиентский компьютер.

  Считается, что компьютер работает в оперативном режиме, если он подключен к контроллеру своего домена. Компьютер считается работающим в автономном режиме, если он не может подключиться к контроллеру своего домена или не является членом какого-либо домена (изолированный компьютер).

- **Подключение кабеля** - Состояние подключения определяется тем, подключен ли сетевой кабель к сетевой карте клиентского компьютера. Это простейший и наименее безопасный способ определить состояние сетевого подключения.

  Считается, что компьютер работает в оперативном режиме, если сетевой кабель подключен к его сетевой карте. Компьютер считается работающим в автономном режиме, если сетевой кабель отключен. Обратите внимание, что учитывается только подключение с помощью кабеля. Беспроводные подключения (Wi-Fi и т.п.) и модемные подключения не учитываются.

Примечание: Самый надежный способ обеспечить безопасное соединение с сервером - проверка подлинности на основе сертификата DeviceLock. В этом случае открытый ключ должен быть установлен на клиентских компьютерах, а секретный (закрытый) ключ - на сервере DeviceLock Enterprise Server.

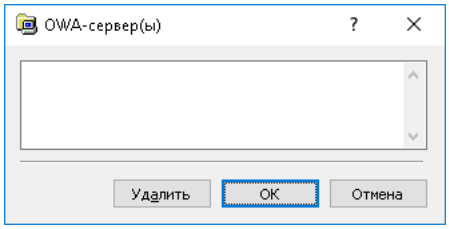
Если открытый ключ сертификата установлен только на клиентских компьютерах, сервер будет отклонять соединения и клиентские компьютеры будут работать в автономном режиме. Если установить секретный ключ сертификата только на сервере DeviceLock Enterprise Server, то и клиент, и сервер пройдут проверку подлинности, как только соединение будет установлено. Однако такая проверка менее безопасна, чем основанная на сертификате проверка подлинности клиента и сервера. Подробнее о сертификатах DeviceLock см. в разделе Сертификаты DeviceLock.

Дополнительную информацию и инструкции по управлению политиками DeviceLock для автономного режима см. в разделе Политики безопасности DeviceLock (офлайн-профиль).

OWA-сервер(ы)

Этот параметр используется, чтобы задать список адресов серверов Outlook Web App (OWA, ранее называвшийся Outlook Web Access). Указанные в этом параметре OWA-серверы трактуются модулем NetworkLock как протокол Web Mail. Все остальные OWA-серверы, не перечисленные здесь, трактуются модулем NetworkLock как протокол HTTP. Данный параметр требует, чтобы была задана политика NetworkLock (любые параметры DeviceLock, связанные с протоколами). В противном случае этот параметр не действует.

Примечание: Серверы outlook.office.com и outlook.office365.com всегда считаются серверами OWA.



Если адресов несколько, их следует разделять запятой (,) или точкой с запятой (;). Также можно нажимать клавишу ENTER после ввода каждой строчки. В адресе допускаются знаки подстановки, такие как звездочка (*) (например, `*.com/owa` означает любой сервер, адрес которого заканчивается на `.com/owa`).

Применять контентно-зависимые правила для имен файлов/папок

Этот параметр позволяет включить или отключить проверку имен файлов и папок с помощью контентно-зависимых правил. Включая этот параметр, примите во внимание следующее:

- Для имен файлов и папок применяются только правила, основанные на группах **Шаблон** и **Ключевые слова**.
- Правила применяются к полному пути файла, включая имя файла и все имена папок.
- Правила срабатывают при чтении, записи или передаче файлов посредством устройств или протоколов, для которых заданы контентно-зависимые правила.
- Если контентно-зависимые правила не заданы для каких-либо действий с файлами, то данный параметр не влияет на выполнение таких действий.

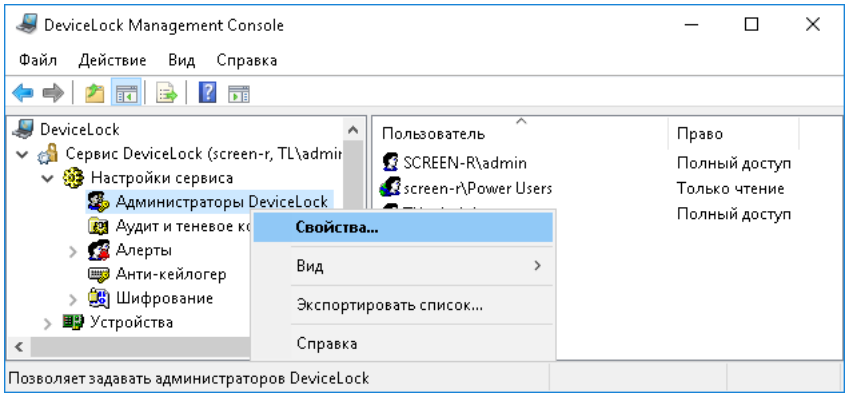
Сервер EtherSensor

В диалоговом окне для этого параметра укажите имя компьютера, на котором работает сервер EtherSensor. Это может быть короткое имя, полное доменное имя или IP-адрес компьютера. Рядом с именем компьютера укажите номер порта EtherSensor в следующем формате: `имя компьютера[номер порта]`. Пример: `MyServer[8080]`

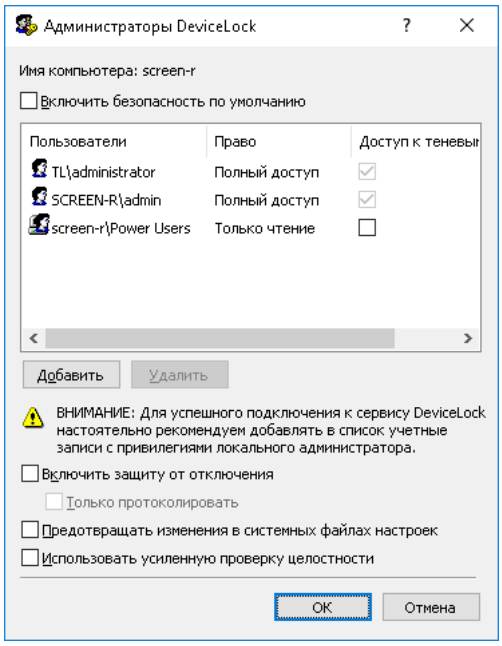
Данный параметр позволяет DeviceLock ассоциировать пользователей с объектами данных приложения (сообщениями, файлами и т. д.), перехваченными модулем EtherSensor. С помощью этого параметра EtherSensor может распознавать в сети объекты, связанные с пользователями компьютера, на котором работает сервис DeviceLock. Подробнее о модуле EtherSensor см. на сайте DeviceLock: devicelock.com/ru/products/network-hybrid-dlp.html.

Администраторы DeviceLock

Эти настройки позволяют определить список учетных записей с административными правами доступа к сервису DeviceLock.



В контекстном меню элемента **Администраторы DeviceLock** выберите команду **Свойства**, чтобы открыть диалоговое окно с настройками.



Стандартная защита основана на списке управления доступом (ACL) Windows. Пользователь без локальных административных привилегий не может подключиться к сервису DeviceLock, изменить его настройки или удалить его. Все это контролируется подсистемой безопасности Windows.

Для включения стандартной защиты, основанной на ACL, установите флажок **Включить безопасность по умолчанию**.

Примечание: Как указано в разделе Правила обеспечения безопасности данного руководства, не рекомендуется наделять обычных пользователей административными привилегиями.

Пользователи с правами локального администратора (члены локальной группы Администраторы) могут подключаться к сервису DeviceLock, используя консоль управления и изменять настройки разрешений, аудита и другие параметры. Более того, такие пользователи могут удалить DeviceLock со своих компьютеров, отключить или остановить сервис DeviceLock, изменить значения ключей реестра агента, удалить исполняемый файл агента и так далее. Другими словами, пользователи с правами локального администратора могут обойти стандартную систему защиты, основанную на ACL.

Однако, даже если пользователи вашей сети имеют административные привилегии на локальных компьютерах, DeviceLock способен обеспечить необходимый уровень защиты. Когда защита DeviceLock включена, никто, исключая авторизованных администраторов, не может подключаться к сервису DeviceLock, останавливать или удалять его. Даже члены локальной группы Администраторы (если они не входят в список авторизованных администраторов DeviceLock) не могут обойти защиту DeviceLock.

Для включения защиты DeviceLock снимите флажок **Включить безопасность по умолчанию**.

Затем вам необходимо определить авторизованные учетные записи (пользователей и/или группы), которые могут администрировать сервис DeviceLock. Для того чтобы добавить нового пользователя или группу в список авторизованных учетных записей, нажмите кнопку **Добавить**. Вы можете добавить несколько учетных записей одновременно.

Для удаления учетных записей из списка используйте кнопку **Удалить**. Используя клавиши Ctrl и/или Shift, вы сможете выделить и удалить несколько записей одновременно.

Чтобы определить, какие действия разрешены пользователю или группе, выберите желаемый уровень доступа:

- **Полный доступ** - Полный доступ позволяет изменять разрешения, аудит и другие параметры, удалять или обновлять сервис DeviceLock.
- **Изменение** - Доступ на изменение позволяет изменять настройки, устанавливать и удалять сервис DeviceLock, но не позволяет добавлять новые учетные записи в список администраторов DeviceLock или изменять права учетных записей, уже имеющихся в этом списке.
- **Только чтение** - Доступ только на чтение позволяет просмотр разрешений, аудита и других параметров. Пользователи и группы с этим уровнем доступа могут просматривать установленные параметры, но не могут ничего изменять или удалять/обновлять сервис DeviceLock.

Для пользователей и групп с уровнем доступа **Изменение** или **Только чтение** можно выбрать опцию **Доступ к теневым копиям**, чтобы обеспечить доступ к теневым копиям и записям активности пользователей. Пользователи и группы, для которых выбрана эта опция, могут просматривать, открывать и сохранять теневые копии и записи активности пользователей из журналов сервиса DeviceLock, используя средства просмотра журнала теневого копирования (см. Просмотрщик журнала теневого копирования (для компьютера)) и журнала активности пользователей (см. Просмотр активности пользователей).

Примечание: Администраторам сервиса DeviceLock, не имеющим доступа к теневым копиям, недоступно содержимое теневых копий и записей активности пользователей. Они не могут открывать, просматривать и сохранять теневые копии и записи активности пользователей.

Настоятельно рекомендуется предоставить администраторам сервиса DeviceLock права локального администратора, поскольку при установке, обновлении или удалении сервиса DeviceLock может потребоваться доступ к диспетчеру управления службами Windows (Service Control Manager) и к общим сетевым ресурсам.

Вот пример правильной настройки списка администраторов сервиса DeviceLock: добавьте в список группу “Администраторы домена” с правом **Полный доступ**. Группа “Администраторы домена” является членом локальной группы “Администраторы” на каждом компьютере домена, все члены группы “Администраторы домена” будут иметь полный доступ к сервису DeviceLock на каждом компьютере. При этом другие члены локальной группы “Администраторы” не смогут администрировать сервис DeviceLock или отключать его.

Установите флажок **Включить защиту от отключения**, чтобы защититься от программ обнаружения и удаления руткитов, которые могут быть злонамеренно использованы для отключения сервиса DeviceLock. Когда защита включена, DeviceLock контролирует целостность своего кода, и любая попытка нарушить целостность кода DeviceLock будет приводить к критической ошибке Windows (BSOD).

Внимание: Некоторые антивирусы, брандмауэры и другое низкоуровневое программное обеспечение сторонних производителей может конфликтовать с защитой от антируткитов, что может вызывать критическую ошибку Windows (BSOD). Рекомендуется включать этот вид защиты только после предварительного тестирования системы.

Установите флажок **Только протоколировать**, чтобы DeviceLock при попытках нарушения целостности его кода только протоколировал такие попытки в журнале аудита, без генерации критической ошибки Windows (BSOD).

Установите флажок **Предотвращать изменения в системных файлах настроек**, чтобы сервис DeviceLock автоматически защищал файл Hosts в Windows.

Примечание: Поскольку DeviceLock использует для разрешения имен локальный файл Hosts, злоумышленник с правами локального администратора может изменить этот файл, чтобы обойти политику безопасности DeviceLock. В целях безопасности рекомендуется защитить файл Hosts с помощью функции **Предотвращать изменения в системных файлах настроек**.

Кроме того, установив или сняв флажок **Использовать усиленную проверку целостности**, вы можете задать тип проверок целостности. Определить повреждения в исполняемых файлах сервиса DeviceLock можно двумя способами:

- Простая проверка целостности: сервис DeviceLock проверяет версии всех исполняемых файлов. Чтобы выбрать этот тип проверки, снимите флажок **Использовать усиленную проверку целостности**.
- Усиленная проверка целостности: сервис DeviceLock проверяет цифровые подписи всех исполняемых файлов. Чтобы выбрать этот тип проверки, установите флажок **Использовать усиленную проверку целостности**. Усиленная проверка целостности занимает больше времени, чем простая проверка.

Рекомендации

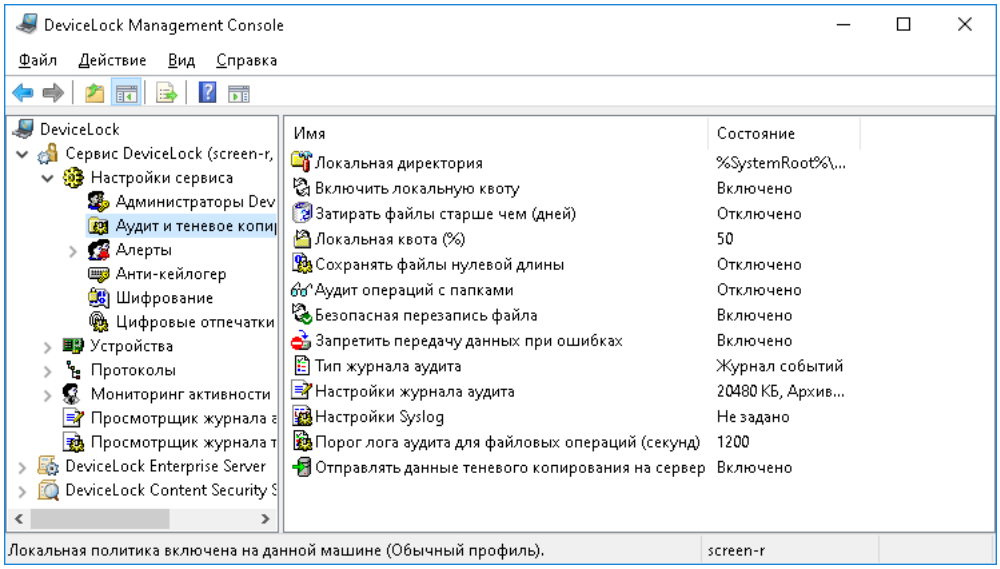
При отключенной безопасности по умолчанию и заданном списке администраторов DeviceLock, доступ к сетевым дискам и физическим портам на клиентском компьютере может быть неожиданно заблокирован независимо от действующих прав доступа. Побочным эффектом является отсутствие сервиса DeviceLock (dlservice) в списке процессов Диспетчера задач.

Такое поведение является частью защиты от администраторов, которые имеют полный доступ к клиентскому компьютеру, но не включены в список администраторов DeviceLock. В случае неожиданной остановки сервиса DeviceLock таким образом блокируется доступ к устройствам и сетевым протоколам во избежание возможной утечки данных.

Для восстановления настроек доступа DeviceLock перезагрузите компьютер. При повторном появлении проблемы попробуйте отключить антивирусное программное обеспечение, которое могло бы вызвать принудительную остановку сервиса DeviceLock.

Аудит и теневое копирование

Эти настройки позволяют задать дополнительные параметры теневого копирования и аудита в сервисе DeviceLock.



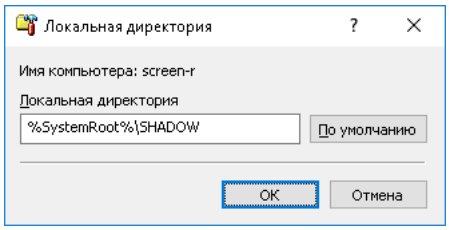
Используйте контекстное меню, которое появляется по нажатию правой кнопки мыши на каждом параметре.

Предусмотрены следующие параметры аудита и теневого копирования:

- Локальная директория
- Порог лога аудита для файловых операций (секунд)
- Включить локальную квоту
- Затирать файлы старше чем (дней)
- Локальная квота (%)
- Сохранять файлы нулевой длины
- Аудит операций с папками
- Безопасная перезапись файла
- Запретить передачу данных при ошибках
- Тип журнала аудита
- Настройки журнала аудита
- Настройки Syslog
- Отправлять данные теневого копирования на сервер

Локальная директория

Этот параметр позволяет указать, где на локальном жестком диске будут сохраняться кэшированные данные (для аудита/теневого копирования, контентного анализа и очереди тревожных оповещений).



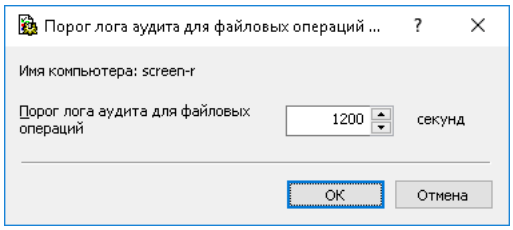
По умолчанию сервис DeviceLock хранит свои кэшированные данные в локальной папке `%SystemRoot%\SHADOW`. Здесь `%SystemRoot%` - это стандартная переменная среды, которая определяет путь до корневой директории Windows (например, `C:\Windows`). Можно указать другую папку на локальном жестком диске.

Сервис DeviceLock защищает свою локальную директорию, так что пользователи не могут получить доступ к файлам внутри этой папки.

Убедитесь, что на диске есть достаточно свободного места (например, если пользователь может скопировать 1 ГБ данных на USB-диск, то это потребует около 2 ГБ на локальном диске). Минимально необходимый размер свободного места на диске - примерно 150 МБ.

Порог лога аудита для файловых операций (секунд)

Этот параметр задает временной порог (в секундах) для объединения повторяющихся событий, связанных с файловыми операциями.



Значение по умолчанию равно 1200 секундам. Если по прошествии этого времени повторяющиеся события не будут зафиксированы, то несколько повторяющихся событий будут объединены в одно сводное событие при выполнении следующих условий:

- События связаны с одним и тем же пользователем.
- События связаны с одним и тем же процессом.
- События связаны с одной и той же файловой операцией (чтение, запись и т. д.).

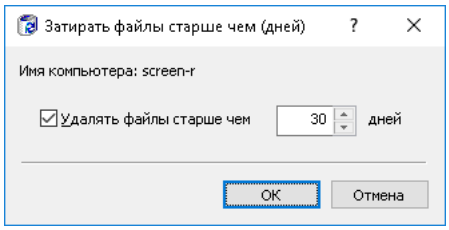
Включить локальную квоту

Этот параметр используется, чтобы включить или отключить автоматическую очистку локально сохраненных кэшированных данных (для теневого копирования и контентного анализа).

Когда этот параметр включен, появляется возможность задавать параметры Затирать файлы старше чем (дней) и Локальная квота (%).

Затирать файлы старше чем (дней)

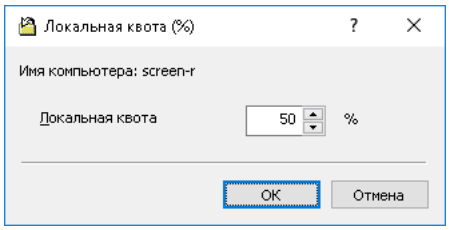
Этот параметр позволяет задать количество дней, которое должно пройти, прежде чем кэшированные данные (для аудита, теневого копирования, контентного анализа и очереди тревожных оповещений) могут быть автоматически удалены из локального хранилища.



Установите флажок **Удалять файлы старше чем** и задайте количество дней.

Локальная квота (%)

Этот параметр позволяет задать дисковую квоту для кэшированных данных, таких как данные аудита, теневые копии, записи мониторинга активности пользователей, данные для анализа содержимого файлов и сообщений, а также данные очереди оповещений.



В поле **Локальная квота** задайте максимальный размер в процентах (от 5 до 100) свободного места на локальном диске, которое может быть выделено для кэшированных данных.

Если квота не установлена (параметр Включить локальную квоту отключен), используется все свободное место на диске, указанном в параметре Локальная директория.

Когда размер папки, заданной параметром Локальная директория, превышает квоту, сервис DeviceLock либо начинает удалять старые данные (если включен параметр Затирать файлы старше чем (дней)), либо прекращает выполнять теневое копирование и контентный анализ (если параметр Затирать файлы старше чем (дней) отключен или нет данных, которые можно удалить). В случае превышения квоты мониторинг активности пользователей также временно прекращается.

Сохранять файлы нулевой длины

Включите этот параметр, чтобы разрешить теневое копирование для файлов нулевой длины.

Протоколирование файлов нулевой длины может быть необходимо, поскольку даже если файл не содержит данных, существует возможность передать информацию (размером до нескольких килобайт) в его имени и пути.

Аудит операций с папками

Включите этот параметр, чтобы обеспечить регистрацию событий, связанных с операциями над папками, такими как создание (запись), переименование, чтение (открытие) и удаление папок. Если этот параметр отключен, все события, связанные с операциями над папками, исключаются из аудита.

Безопасная перезапись файла

Включите этот параметр, чтобы предотвратить удаление исходного файла в результате попыток пользователя заменить его на файл с тем же именем и запрещенным содержимым. Когда этот параметр включен, исходный файл остается в папке без изменений, если его перезапись была запрещена контентно-зависимыми правилами. Событие восстановления исходного файла регистрируется в журнале аудита.

Примечание: Если этот параметр включен и при этом действуют какие-либо запрещающие запись контентно-зависимые правила, удаление файлов может занять больше времени, чем обычно.

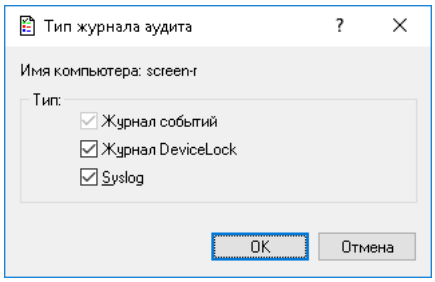
Запретить передачу данных при ошибках

Включите этот параметр, чтобы запретить передачу данных, если невозможно обеспечить их теневое копирование или контентный анализ. В результате пользователи смогут передавать данные только при условии, что на диске имеется достаточно свободного пространства для создания теневых копий и сохранения данных, которые необходимы для нормальной работы контентно-зависимых правил.

Если включен параметр **Запретить передачу данных при ошибках**, превышена квота, заданная параметром Локальная квота (%), и нет данных, которые можно удалить, то сервис DeviceLock прекращает теневое копирование и контентный анализ, блокируя любые попытки пользователя передать данные.

Тип журнала аудита

Этот параметр позволяет указать журналы для записи данных аудита.

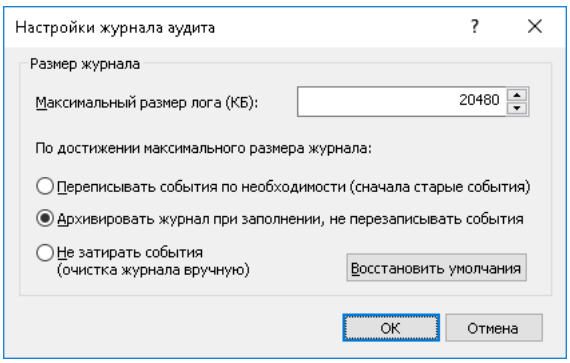


Предусмотрены следующие варианты:

- **Журнал событий** - Данные аудита записываются в стандартный журнал событий Windows, хранящийся на локальном компьютере.
- **Журнал DeviceLock** - Данные аудита записываются в защищенный закрытый журнал. Данные из этого журнала передаются на сервер DeviceLock Enterprise Server для централизованного хранения в базе данных.
- **Syslog** - Данные аудита записываются на сервер syslog.

Настройки журнала аудита

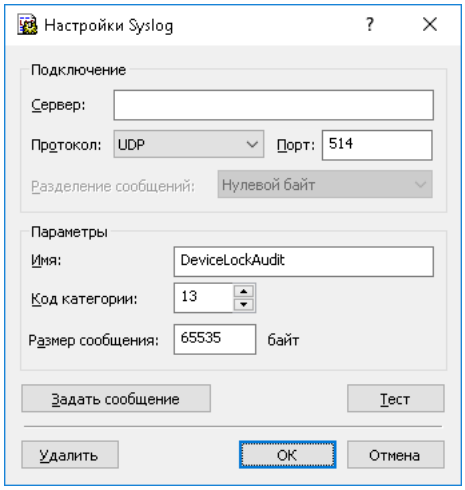
Этот параметр используется, чтобы определить максимальный размер журнала аудита и правила его перезаписи.



Подробное описание настроек журнала аудита см. в разделе Настройки журнала аудита (для компьютера).

Настройки Syslog

Этот параметр используется для настройки доступа к серверу syslog.



- **Подключение** - Введите информацию о сервере syslog:
  - **Сервер** - Доменное имя или IP адрес сервера syslog.
  - **Протокол** - Протокол доступа к серверу syslog, **TCP** или **UDP**. По умолчанию выбран протокол **UDP**.
  - **Порт** - Номер порта для доступа к серверу syslog. По умолчанию указан порт **514**.
  - **Разделение сообщений** - Способ формирования сообщений для протокола **TCP**. Можно выбрать: **Нулевой байт**, **LF**, **CR+LF** или **Длина сообщения**.
- **Параметры** - Задайте следующие параметры подключения:
  - **Имя** - Уникальное имя для канала связи с сервером syslog (имя по умолчанию - DeviceLockAudit).
  - **Код категории** - Одно из стандартных значений сервера syslog (от 0 до 23) для указания типа программы, которая записывает сообщения в журнал.
  - **Размер сообщения** - Размер syslog-сообщения, в байтах (65535 по умолчанию).

- **Задать сообщение** - Настройте шаблон сообщений журнала syslog для целей аудита. Описание шаблона см. в разделе Настройки алертов: Syslog.

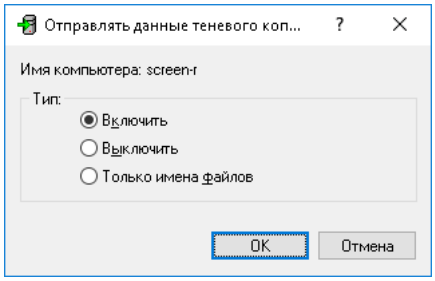
  В диалоговом окне **Syslog-сообщение для аудита**, которое открывается по нажатию кнопки **Задать сообщение**, можно также:

  - Выбрать степень серьезности сообщения из списка **Уровень**.
  - Загрузить шаблон сообщения из текстового файла, использующего символы табуляции в качестве разделителя. Нажмите кнопку **Загрузить,** и выберите файл. Будет загружено все содержимое файла.
  - Восстановить шаблон по умолчанию. Для этого нажмите кнопку **Восстановить умолчания**.

- **Удалить** - Нажмите эту кнопку, чтобы удалить все значения параметров и установить значения параметров по умолчанию.
- **Тест** - Нажмите эту кнопку, чтобы проверить настройку доступа к журналу syslog путем отправки тестовых данных. Если параметры доступа указаны правильно, консоль сообщает об успешной отправке тестовых данных. В противном случае, консоль выдает сообщение с описанием проблемы.

Отправлять данные теневого копирования на сервер

Этот параметр используется для настройки передачи данных теневого копирования и сеансов мониторинга активности пользователей на сервер DeviceLock Enterprise Server.



Предусмотрены следующие варианты настройки:

- **Включить** - На сервер DeviceLock Enterprise Server передаются все данные теневого копирования и записи сеансов мониторинга активности пользователей.
- **Выключить** - Данные теневого копирования и записи сеансов мониторинга активности пользователей сохраняются на клиентском компьютере без передачи на сервер. На сервер передаются только данные аудита из собственного журнала DeviceLock (если он используется).
- **Только имена файлов** - На сервер передаются только имена файлов теневого копирования (но не сами файлы). Файлы теневого копирования сохраняются на клиентском компьютере. Их можно передать позже, выбрав для параметра **Отправлять данные теневого копирования на сервер** вариант настройки **Включить**.

  Если выбран вариант настройки **Только имена файлов**, на сервер передается только информация о сеансах мониторинга активности пользователей, а записи сеансов сохраняются на клиентском компьютере. Их можно передать на сервер позже, выбрав для данного параметра вариант настройки **Включить**.

Внимание: Если на сервер были переданы только имена файлов теневого копирования и затем файлы были удалены в журнал удаленных данных теневого копирования, то при выборе варианта **Включить** для параметра **Отправлять данные теневого копирования на сервер** эти файлы теневого копирования не будут переданы на сервер; кроме того, они будут удалены с клиентского компьютера.

Алерты

Администратор DeviceLock может настроить автоматическую рассылку тревожных оповещений (алертов), чтобы оперативно получать информацию об инцидентах, событиях или проблемах. Оповещения в реальном времени упрощают отслеживание и регистрацию событий в журнале, а также позволяют своевременно реагировать на происшествия и нарушения правил.

DeviceLock поддерживает следующие типы тревожных оповещений:

- Оповещения о том, что определенный пользователь пытается получить доступ к устройству определенного типа или к протоколу.
- Оповещения о том, что сработало контентно-зависимое правило.
- Оповещения о том, что сработало правило Базового IP-файрвола.
- Административные оповещения. Оповещения администратора о происшествиях в окружении DeviceLock, такие как **Оповещать при изменении политик агента**, **Оповещать при повреждении политик агента** и многие другие.

Оповещения могут отправляться адресатам по электронной почте или через SNMP-уведомления. Кроме того, оповещения могут отправляться на сервер syslog.

Перед настройкой тревожных оповещений DeviceLock выполните следующее:

- Выберите способ доставки оповещений - через SNMP-уведомления, по электронной почте или через syslog.
- Чтобы получать оповещения через SNMP-уведомления, настройте в сервисе DeviceLock поддержку SNMP и укажите SNMP-сервер (см. Настройки алертов: SNMP).

  Примечание: Здесь и далее предполагается, что вы знакомы с протоколом SNMP (Simple Network Management Protocol) и соответствующими принципами управления.

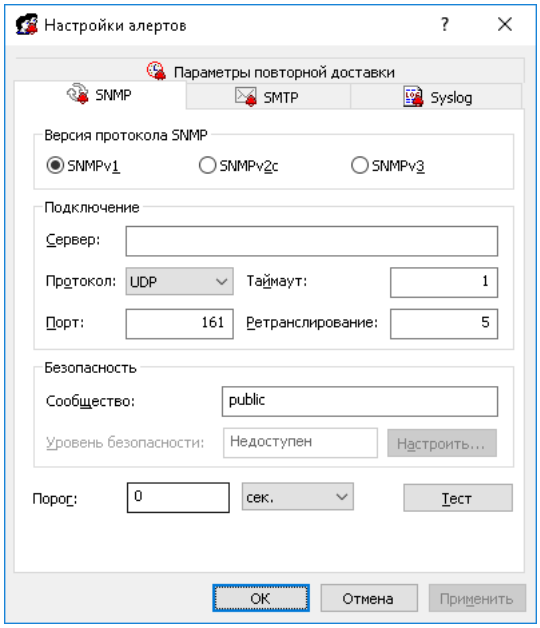
- Чтобы получать оповещения по электронной почте, настройте почтовые уведомления, указав SMTP-сервер, настройки уведомления и шаблон письма (см. Настройки алертов: SMTP).
- Чтобы получать оповещения через syslog, настройте отправку сообщений на сервер syslog (см. Настройки алертов: Syslog).

  Примечание: Здесь и далее предполагается, что вы знакомы с протоколом syslog и соответствующими принципами управления.

- Настройте параметры при сбое доставки уведомлений, в том числе количество и периодичность попыток отправки, а также срок хранения не доставленного сообщения в очереди на отправку (см. Настройки алертов: Параметры повторной доставки).
- Включите уведомления об интересующих вас событиях. При включении уведомлений о специальных событиях необходимо указать условия, при которых уведомление будет отправляться. Информацию о включении административных оповещений см. в разделе Административные алерты. Информацию о включении оповещений для устройств см. в разделе Аудит, теневое копирование и алерты (обычный профиль). Информацию о включении оповещений для протоколов см. в разделе Аудит, теневое копирование и алерты для протоколов. Информацию о включении оповещений для контентно-зависимых правил см. в разделах Создание правил для устройств и Создание правил для протоколов. Информацию о включении оповещений для определенного правила Базового IP-файрвола см. в разделе Базовый IP-файрвол и Создание правил файрвола.

Настройки алертов: SNMP

На вкладке **SNMP** диалогового окна **Настройки алертов** можно настроить поддержку SNMP в сервисе DeviceLock.



Чтобы открыть это диалоговое окно, выполните одно из следующих действий:

- В дереве консоли щелкните правой кнопкой мыши **Алерты** и выберите **Управление**.
- В дереве консоли выберите **Алерты** и нажмите **Управление** на панели инструментов.
- В дереве консоли выберите **Алерты**, а затем на панели сведений щелкните правой кнопкой мыши **SNMP** и выберите **Управление**.
- В дереве консоли выберите **Алерты**, а затем на панели сведений дважды щелкните **SNMP**.

Примечание: Можно задать различные параметры тревожных оповещений для оперативного и автономного режимов. Настройки оперативного режима (обычный профиль) применяются к клиентским компьютерам, находящимся в сети. Настройки автономного режима (офлайн-профиль) применяются к клиентским компьютерам, работающим автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Дополнительную информацию о политиках DeviceLock для автономного режима работы см. в разделе Политики безопасности DeviceLock (офлайн-профиль).

DeviceLock поддерживает протоколы SNMPv1, SNMPv2c и SNMPv3. Можно настроить сервис DeviceLock на автоматическую рассылку оповещений на указанный SNMP-сервер при возникновении условий срабатывания. Данные оповещения отправляются только при соблюдении следующих условий:

- SNMP-сервер настроен на получение SNMP-уведомлений (SNMP traps).
- Удаленный компьютер, на котором работает SNMP-сервер, доступен со всех компьютеров, где установлен сервис DeviceLock.
- Включена рассылка оповещений через SNMP-уведомления.

Заполните вкладку **SNMP** следующим образом:

- **Версия протокола SNMP** - Настройте сервис DeviceLock на использование той версии SNMP, которая поддерживается вашим SNMP-сервером. Возможные варианты: **SNMPv1**, **SNMPv2c** и **SNMPv3**.
- **Подключение** - Укажите информацию об SNMP-сервере:
  - **Сервер** - SNMP-сервер, на который будут отправляться уведомления. В поле **Сервер** введите имя узла или IP-адрес SNMP-сервера.
  - **Протокол** - Транспортный протокол для передачи данных между сервисом DeviceLock и SNMP-сервером. Возможные варианты: **UDP** и **TCP**.
  - **Таймаут** - Промежуток времени, в течение которого сервис DeviceLock ожидает ответа от SNMP-сервера (в секундах) перед повторной отправкой пакета данных. Значение по умолчанию равно **1** секунде.
  - **Порт** - Порт, по которому SNMP-сервер должен получать SNMP-уведомления. По умолчанию используется порт **161**.
  - **Ретранслирование** - Количество повторных запросов от сервиса DeviceLock на SNMP-сервер, если сервер не отвечает. По умолчанию выполняется **5 попыток**. Это значение задается только для TCP-подключений.
- **Безопасность** - Задайте настройки безопасности SNMP:
  - **Сообщество** - Имя группы SNMP для аутентификации на SNMP-сервере. Значение по умолчанию: **public**. Применимо только для SNMPv1 и SNMPv2c.
  - **Имя пользователя** - Имя пользователя для аутентификации на SNMP-сервере. Применимо только для SNMPv3. Если аутентификация не требуется, имя пользователя можно не задавать.
  - **Имя контекста** - Имя контекста указывается, если SNMP-сервер требует контекст SNMP. Применимо только для SNMPv3.
  - **ID контекстного движка** - Идентификатор контекстного движка, если SNMP-сервер требует контекст SNMP. Применимо только для SNMPv3.
  - **Протокол аутентификации** - Протокол для шифрования аутентификации на SNMP-сервере. Применимо только для SNMPv3. Возможные варианты:
    - **Нет** (соответствует уровню безопасности SNMP **Нет защиты** - Взаимодействие без аутентификации и шифрования).
    - **HMAC-SHA** (соответствует уровню безопасности SNMP **Аутентификация**)
  - **Пароль/ Подтверждение пароля** - Пароль учетной записи, используемой для аутентификации на SNMP-сервере. Применимо только для SNMPv3.
  - **Протокол конфиденциальности** - Протокол шифрования данных при взаимодействии с SNMP. Применимо только для SNMPv3. Возможные варианты:
    - **Нет** (соответствует уровню безопасности SNMP **Аутентификация** - Взаимодействие с аутентификацией и без шифрования).
    - **CBC-AES-128** (соответствует уровню безопасности SNMP **Аутентификация и конфиденциальность** - Взаимодействие с аутентификацией и шифрованием).
  - **Пароль/ Подтверждение пароля** - Пароль для шифрования данных. Применимо только для SNMPv3.
- **Порог** - Задайте временной интервал (в часах, минутах или секундах) для объединения событий при отправке оповещений. Сервис DeviceLock объединяет события, произошедшие в течение порогового времени, и создает объединенное событие при выполнении следующих условий:

  a) События относятся к одному типу (**Успех**, **Отказ** или **Информация**).

b) События регистрируются для одного и того же типа устройств/протокола.

c) События связаны с одним и тем же пользователем.

d) События связаны с одним и тем же PID.

Значение по умолчанию - `0` секунд.

> **Примечание:** При отправке оповещений сервис DeviceLock объединяет только события, связанные с доступом. Административные оповещения не объединяются.

- **Тест** - Отправьте тестовое SNMP-оповещение, чтобы проверить правильность настройки сервиса DeviceLock. В результате тестовой операции отобразится одно из двух сообщений:
  - Тест может быть выполнен успешно, т.е. пробное SNMP-оповещение было отправлено с настроенными для него параметрами. В этом случае сообщение будет следующим: "Тестовый алерт SNMP успешно отправлен."
  - Тест может быть не выполнен, т.е. пробное SNMP-оповещение отправить не удалось. В этом случае сообщение будет следующим: "Тестовый алерт SNMP не был отправлен из-за ошибки: <описание ошибки>."

SNMP-уведомления от сервиса DeviceLock представляются в формате MIB (Management Information Base). MIB для сервиса DeviceLock имеет идентификатор объекта (OID) `1.3.6.1.4.1.60000` или `iso.org.dod.internet.private.enterprise.DeviceLock` и содержит следующие узлы:

- `products(1)`
- `agent(1)`
- `alerts(1)` - Этот узел содержит по одному экземпляру каждого из следующих MIB-объектов:
  - `eventType(1)` - Класс события (Успех для разрешенной попытки доступа, Отказ для запрещенной попытки, Информация для событий срабатывания контентно-зависимых правил обнаружения содержимого). Обратите внимание, что значение `eventType` отображается в виде числа, а не строки: `8` означает успешную попытку, `16` - отказ, а `4` означает событие обнаружения содержимого.
  - `eventId(2)` - Номер, идентифицирующий определенный тип событий.
  - `userSid(3)` - Идентификатор безопасности (SID) пользователя, связанного с данным событием.
  - `userName(4)` - Имя пользователя, связанного с данным событием.
  - `computerName(5)` - Имя компьютера, от которого получено событие.
  - `processId(6)` - Идентификатор процесса, связанного с данным событием.
  - `processName(7)` - Имя процесса, связанного с данным событием.
  - `source(8)` - Тип устройства или протокола, связанного с данным событием. Значение `source` отображается в виде числа, а не строки. Используются следующие числовые значения:

Устройства	**Протоколы**
`1` - Гибкий диск	`513` - ICQ Messenger
`2` - Съемные устройства	`514` - HTTP
`3` - Жесткий диск	`515` - Торрент
`5` - Оптический привод	`516` - FTP
`7` - Последовательный порт	`517` - SMTP

Устройства	Протоколы
8 - Параллельный порт	520 - Jabber
9 - Ленточные накопители	521 - IRC
10 - USB-порт	522 - Telnet
11 - ИК-порт	524 - Mail.ru Агент
12 - FireWire-порт	525 - Web-почта
13 - Bluetooth	526 - Социальные сети
14 - WiFi	527 - SSL
15 - Windows Mobile	528 - SMB
16 - Palm	529 - MAPI
17 - Принтер	530 - Файловые хранилища
18 - iPhone-устройства	531 - Skype
19 - BlackBerry-устройства	533 - Любой (TCP)
20 - Буфер обмена	534 - Любой (UDP)
21 - TC-устройства	539 - IP (TCP)
22 - MTP	540 - IP (UDP)
	541 - IBM Notes
	542 - WhatsApp
	546 - Telegram
	547 - Viber
	548 - Tor-браузер
	549 - Web-поиск
	550 - Поиск работы
	551 - Zoom

- `action(9)` - Тип действия пользователя.
- `name(10)` - Имя объекта (файл, USB-устройство и т. д.).
- `info(11)` - Прочая информация об устройстве, связанном с событием, например флаги доступа, имена устройств и так далее.
- `reason(12)` - Причина возникновения события.
- `datetime(13)` - Дата и время получения события (в формате RFC3339) в сервисе DeviceLock.

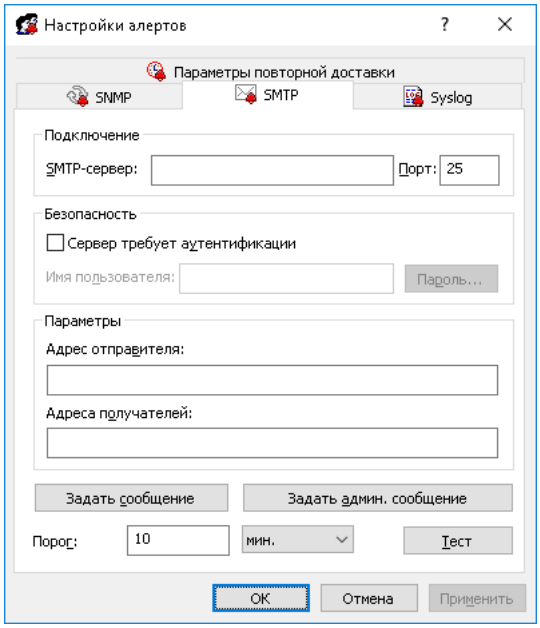
Примечание: Данные MIB-объекты соответствуют полям журнала аудита.

SNMP-уведомление рассылается каждый раз, когда происходит событие, приведшее к тревожному оповещению. Ниже приводится пример SNMP-оповещения.

```
⊟ 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
```

Настройки алертов: SMTP

На вкладке **SMTP** диалогового окна **Настройки алертов** можно настроить отправку уведомления по электронной почте.



Чтобы открыть это диалоговое окно, выполните одно из следующих действий:

- В дереве консоли щелкните правой кнопкой мыши **Алерты** и выберите **Управление**.
- В дереве консоли выберите **Алерты** и нажмите **Управление** на панели инструментов.
- В дереве консоли выберите **Алерты**, а затем на панели сведений щелкните правой кнопкой мыши **SMTP** и выберите **Управление**.
- В дереве консоли выберите **Алерты**, а затем на панели сведений дважды щелкните **SMTP**.

Примечание: Можно настроить различные параметры тревожных оповещений для оперативного и автономного режимов. Настройки оперативного режима (обычный профиль) применяются к клиентским компьютерам, находящимся в сети. Настройки автономного режима (офлайн-профиль) применяются к клиентским компьютерам, работающим автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Для получения дополнительной информации о политиках DeviceLock для автономного режима работы, см. раздел Политики безопасности DeviceLock (офлайн-профиль).

Для передачи тревожных оповещений посредством почтовых сообщений DeviceLock использует протокол SMTP. Можно настроить сервис DeviceLock на автоматическую рассылку тревожных оповещений на указанные адреса электронной почты при возникновении условий срабатывания. Для настройки почтовых оповещений выполните следующее:

1. Укажите SMTP-сервер и настройки почтовых уведомлений.
2. Задайте шаблоны почтовых сообщений.

DeviceLock поставляется с набором готовых шаблонов, которые можно использовать для формирования тревожных сообщений. Эти шаблоны определяют основное содержимое, формат и структуру почтовых уведомлений. Предусмотрены следующие шаблоны:

- Шаблон сообщения для административных оповещений.
- Шаблон сообщения для всех остальных оповещений.

Каждый шаблон содержит следующие данные:

- **Тема письма** - Текст в строке **Тема** почтового сообщения. Текст по умолчанию для административных оповещений: “Административный алерт DeviceLock”. Текст по умолчанию для всех остальных оповещений: “Алерт DeviceLock”.
- **Тело письма** - Текст почтового сообщения. DeviceLock может отправлять сообщение как в виде простого текста, так и в формате HTML. Текст сообщения совпадает в обоих шаблонах и включает в себя статичный текст и макросы. Статичный текст по умолчанию: “Зарегистрировано следующее событие”. В строку **Тема** и/или в текст сообщения можно вставить дополнительные сведения, используя следующие стандартные макросы:
    - `%EVENT_TYPE%` - Класс события (**Успех** для разрешенной попытки доступа, **Отказ** для запрещенной попытки доступа, **Информация** для прочих событий).
    - `%COMP_NAME%` - Имя компьютера, от которого получено событие.
    - `%COMP_FQDN%` - Полное доменное имя компьютера, от которого получено событие.
    - `%COMP_IP%` - Список всех IP-адресов компьютера, разделенных запятой.
    - `%DATE_TIME%` - Дата и время, когда событие было получено сервисом DeviceLock. Дата и время указываются в соответствии с региональными и языковыми настройками на клиентском компьютере.
    - `%SOURCE%` - Тип устройства или протокола, с которым связано событие.
    - `%ACTION%` - Тип действия пользователя.
    - `%NAME%` - Имя объекта (файла, USB-устройства и т.п.).
    - `%INFO%` - Прочая информация об устройстве, связанном с событием, например флаги доступа, название устройства и так далее.
    - `%REASON%` - Причина возникновения события.
    - `%USER_NAME%` - Имя пользователя, связанного с событием.
    - `%USER_SID%` - Идентификатор безопасности (SID) пользователя, связанного с данным событием.
    - `%PROC_NAME%` - Имя процесса приложения, связанного с данным событием.
    - `%PROC_ID%` - Идентификатор процесса приложения, связанного с событием.
    - `%EVENT_ID%` - Число, идентифицирующее тип события.
    - `%SUMMARY_TABLE%` - Таблица с детализацией отдельных событий для агрегированных алертов.

  Эти макросы заменяются на фактические значения во время создания сообщения.

Заполните вкладку **SMTP** следующим образом:

- **Подключение** - Укажите данные почтового сервера для отправки сообщений:
    - **SMTP-сервер** - Имя узла или IP-адрес SMTP-сервера.
    - **Порт** - Номер порта для отправки сообщений на почтовый сервер. По умолчанию используется порт `25`.

Примечание: Поддерживаются незащищенные и защищенные (SSL) соединения с указанным сервером SMTP. DeviceLock автоматически определяет зашифрованные соединения и их тип.

- **Безопасность** - Задайте параметры безопасности SMTP:
  - **Сервер требует аутентификации** - Тип проверки подлинности для соединения с SMTP-сервером. Установите флажок **Сервер требует аутентификации**, чтобы настроить обычную проверку подлинности. Снимите флажок **Сервер требует аутентификации**, если SMTP-сервер не требует проверку подлинности.
  - **Имя пользователя**, **Пароль** - Имя и пароль пользователя SMTP-сервера нужно указать, если SMTP-сервер требует проверку подлинности.
- **Параметры** - Укажите отправителя и получателей сообщения:
  - **Адрес отправителя** - Почтовый адрес, с которого будут рассылаться оповещения.
  - **Адреса получателей** - Почтовые адреса получателей оповещений о событиях. Если адресов несколько, их следует разделять запятой (,) или точкой с запятой (;).
- **Задать сообщение** - Нажмите эту кнопку, чтобы настроить шаблон сообщений для оповещений.

  В появившемся диалоговом окне **E-mail сообщение для алертов** можно также:
  - Изменить формат всех сообщений с HTML на простой текст или наоборот. Для этого выберите опцию **Текст** или **HTML**, соответственно. По умолчанию почтовые сообщения отправляются в виде простого текста.
  - Загрузить текст сообщения из текстового файла с разделителем-табуляцией (.txt). Для этого нажмите кнопку **Загрузить**. При этом будет загружено все содержимое файла. Содержимое может быть представлено в виде простого текста или HTML.
  - Восстановить настройки по умолчанию. Для этого нажмите кнопку **Восстановить умолчания**.
- **Задать админ. сообщение** - Нажмите эту кнопку, чтобы настроить шаблон сообщений для административных оповещений.

  В появившемся диалоговом окне **E-mail сообщение для административных алертов** можно также:
  - Изменить формат всех сообщений с HTML на простой текст или наоборот. Для этого выберите опцию **Текст** или **HTML**, соответственно. По умолчанию почтовые сообщения отправляются в виде простого текста.
  - Загрузить текст сообщения из текстового файла с разделителем-табуляцией (.txt). Для этого нажмите кнопку **Загрузить**. При этом будет загружено все содержимое файла. Содержимое может быть представлено в виде простого текста или HTML.
  - Восстановить настройки по умолчанию. Для этого нажмите кнопку **Восстановить умолчания**.
- **Порог** - Задайте временной интервал (в часах, минутах или секундах) для консолидации событий при отправке оповещений. Сервис DeviceLock консолидирует события, произошедшие в течение порогового времени, и создает объединенное событие при выполнении следующих условий:

  a) События относятся к одному типу (**Успех**, **Отказ** или **Информация**).

  b) События регистрируются для одного и того же типа устройств/протокола.

  c) События связаны с одним и тем же пользователем.

  d) События связаны с одним и тем же PID.

  Значение по умолчанию - `10` минут.

  Примечание: При отправке уведомлений сервис DeviceLock объединяет только события, связанные с доступом. Административные оповещения не консолидируются.

- **Тест** - Отправьте тестовое сообщение, чтобы проверить правильность настройки. В результате тестовой операции отобразится одно из двух сообщений:
    - Если тест выполнен успешно, т.е. пробное сообщение отправлено с настроенными для него параметрами, сообщение будет следующим: “Тестовый алерт SMTP успешно отправлен.”
    - Если тест не выполнен, т.е. пробное сообщение отправить не удалось, сообщение будет следующим: “Тестовый алерт SMTP не был отправлен из-за ошибки: <описание ошибки>.”

Пример тревожного оповещения, доставленного по электронной почте:

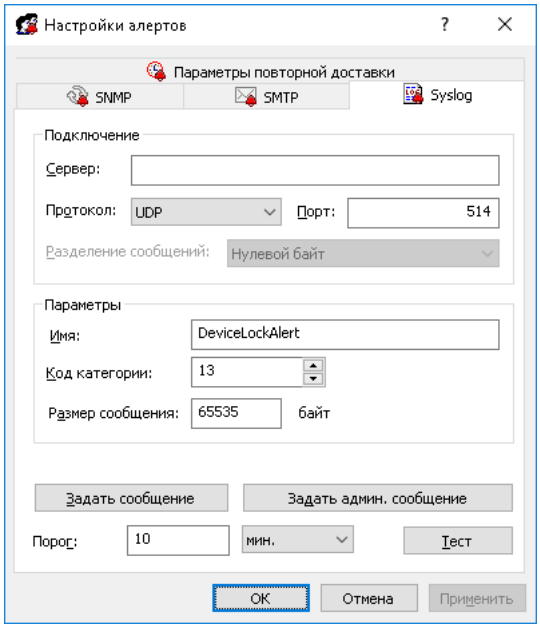
Алерт DeviceLock

Произошло следующее событие:
Тип события: Отказ (16)
Компьютер: WIN7X64
Дата/время: 09/11/12 18:24:38
Источник: Съемные устройства (2)
Действие: Запись
Имя: E:\Market research.docx
Информация:
Причина: Правило: “Закрытые данные” (Совпало: Все ключевые слова)
Имя пользователя: Win7x64\Administrator
SID пользователя: S-1-5-21-3601177953-2830843172-1403898981-500
Имя процесса: C:\Windows\Explorer.exe
Id процесса: 456
Id события: 13

Примечание: Названия полей в почтовом оповещении соответствуют названиям полей в журнале аудита.

Настройки алертов: Syslog

На вкладке **Syslog** диалогового окна **Настройки алертов** можно настроить параметры для отправки оповещений на сервер syslog.



Чтобы открыть это диалоговое окно, выполните одно из следующих действий:

- В дереве консоли щелкните правой кнопкой мыши **Алерты** и выберите **Управление**.
- В дереве консоли выберите **Алерты** и нажмите **Управление** на панели инструментов.
- В дереве консоли выберите **Алерты**, а затем на панели сведений щелкните правой кнопкой мыши **Syslog** и выберите **Управление**.
- В дереве консоли выберите **Алерты**, а затем на панели сведений дважды щелкните **Syslog**.

Примечание: Можно настроить различные параметры тревожных оповещений для оперативного и автономного режимов. Настройки оперативного режима (обычный профиль) применяются к клиентским компьютерам, находящимся в сети. Настройки автономного режима (офлайн-профиль) применяются к клиентским компьютерам, работающим автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Для получения дополнительной информации о политиках DeviceLock для автономного режима работы, см. раздел Политики безопасности DeviceLock (офлайн-профиль).

Можно настроить сервис DeviceLock на автоматическую отправку тревожных оповещений на указанный сервер syslog при возникновении условий срабатывания. Отправка оповещений происходит только при соблюдении следующих условий:

- Сервер syslog настроен и готов к приему оповещений.
- Удаленный компьютер, на котором запущен сервер syslog, доступен со всех компьютеров, на которых работает сервис DeviceLock.
- Настроена отправка тревожных оповещений на сервер syslog.

DeviceLock поставляется с набором готовых шаблонов тревожных оповещений для отправки на сервер syslog. Эти шаблоны определяют основное содержимое, формат и структуру оповещений. DeviceLock предоставляет следующие шаблоны:

- Шаблон сообщения syslog для административных оповещений.
- Шаблон сообщения syslog для прочих оповещений.

Каждый шаблон содержит следующие данные:

- **Тело сообщения** - Текст, отображаемый в теле сообщения syslog. Текст сообщения совпадает в обоих шаблонах и включает в себя статичный текст и макросы. Статичный текст по умолчанию: "Зарегистрировано следующее событие". В тело сообщения можно вставить дополнительные сведения, используя следующие макросы:
    - `%EVENT_TYPE%` - Класс события (**Успех** для разрешенной попытки доступа, **Отказ** для запрещенной попытки доступа, **Информация** для прочих событий).
    - `%COMP_NAME%` - Имя компьютера, от которого получено событие.
    - `%COMP_FQDN%` - Полное доменное имя компьютера, от которого получено событие.
    - `%COMP_IP%` - Список всех IP-адресов компьютера, разделенных запятой.
    - `%DATE_TIME%` - Дата и время, когда событие было получено сервисом DeviceLock. Дата и время указываются в соответствии с региональными и языковыми настройками на клиентском компьютере.
    - `%SOURCE%` - Тип устройства или протокола, с которым связано событие.
    - `%ACTION%` - Тип действия пользователя.
    - `%NAME%` - Имя объекта (файла, USB-устройства и т.п.).
    - `%INFO%` - Прочая информация об устройстве, связанном с событием, например флаги доступа, название устройства и так далее.
    - `%REASON%` - Причина возникновения события.
    - `%USER_NAME%` - Имя пользователя, связанного с событием.
    - `%USER_SID%` - Идентификатор безопасности (SID) пользователя, связанного с данным событием.
    - `%PROC_NAME%` - Имя процесса приложения, связанного с данным событием.
    - `%PROC_ID%` - Идентификатор процесса приложения, связанного с событием.
    - `%EVENT_ID%` - Число, идентифицирующее тип события.
    - `%SUMMARY_TABLE%` - Таблица с детализацией отдельных событий для агрегированных алертов.

  Эти макросы заменяются на фактические значения во время создания сообщения.

Заполните вкладку **Syslog** следующим образом:

- **Подключение** - Введите информацию о сервере syslog:
    - **Сервер** - Доменное имя или IP адрес сервера syslog.
    - **Протокол** - Протокол доступа к серверу syslog, **TCP** или **UDP**. По умолчанию выбран протокол **UDP**.
    - **Порт** - Номер порта для доступа к серверу syslog. Порт по умолчанию - `514`.
    - **Разделение сообщений** - Способ формирования сообщений для протокола **TCP**. Можно выбрать: **Нулевой байт**, **LF**, **CR+LF** или **Длина сообщения**.

- **Параметры** - Задайте следующие параметры подключения:
  - **Имя** - Уникальное имя для канала связи с сервером syslog. По умолчанию используется имя **DeviceLockAlert**.
  - **Код категории** - Одно из стандартных значений сервера syslog (от 0 до 23) для указания типа программы, которая записывает сообщения в журнал.
  - **Размер сообщения** - Размер syslog-сообщения, в байтах. Размер по умолчанию - `65535` байт.
- **Задать сообщение** - Нажмите эту кнопку, чтобы настроить шаблон сообщений syslog для оповещений.

  В появившемся диалоговом окне **Syslog-сообщение для алертов** можно также:
  - Выбрать степень серьезности сообщения из списка **Уровень**.
  - Загрузить шаблон сообщения из текстового файла, использующего символы табуляции в качестве разделителя. Нажмите кнопку **Загрузить,** и выберите файл. Будет загружено все содержимое файла.
  - Восстановить шаблон по умолчанию. Для этого нажмите кнопку **Восстановить умолчания**.
- **Задать админ. сообщение** - Нажмите эту кнопку, чтобы настроить шаблон сообщений syslog для административных оповещений.

  В появившемся диалоговом окне **Syslog-сообщение для административных алертов** можно также:
  - Выбрать степень серьезности сообщения из списка **Уровень**.
  - Загрузить шаблон сообщения из текстового файла, использующего символы табуляции в качестве разделителя. Нажмите кнопку **Загрузить,** и выберите файл. Будет загружено все содержимое файла.
  - Восстановить шаблон по умолчанию. Для этого нажмите кнопку **Восстановить умолчания**.
- **Порог** - Задайте временной интервал (в часах, минутах или секундах) для объединения событий при отправке алертов. Сервис DeviceLock объединяет события, произошедшие в течение порогового времени, и создает объединенное событие при выполнении следующих условий:

  a) События относятся к одному типу (**Успех**, **Отказ** или **Информация**).

  b) События регистрируются для одного и того же типа устройств/протокола.

  c) События связаны с одним и тем же пользователем.

  d) События связаны с одним и тем же PID.

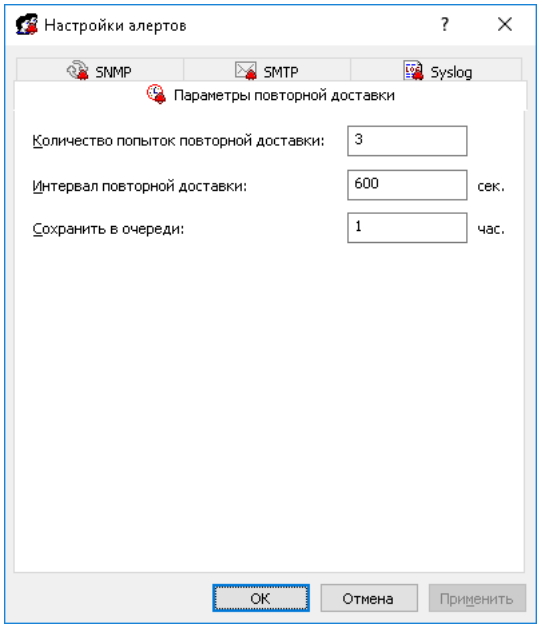
  Значение по умолчанию - `10` минут.

  Примечание: При отправке уведомлений сервис DeviceLock объединяет только события, связанные с доступом. Административные оповещения не объединяются.

- **Тест** - Отправьте тестовое сообщение, чтобы проверить правильность настройки. В результате тестовой операции отобразится одно из двух сообщений:
  - Если тест выполнен успешно, т.е. пробное сообщение отправлено с настроенными для него параметрами, сообщение будет следующим: “Тестовый алерт Syslog успешно отправлен.”
  - Если тест не выполнен, т.е. пробное сообщение отправить не удалось, сообщение будет следующим: “Тестовый алерт Syslog не был отправлен из-за ошибки: <описание ошибки>.”

Настройки алертов: Параметры повторной доставки

На вкладке **Параметры повторной доставки** диалогового окна **Настройки алертов** можно настроить действия при сбое отправки тревожного оповещения.



Чтобы открыть это диалоговое окно, выполните одно из следующих действий:

- В дереве консоли щелкните правой кнопкой мыши **Алерты** и выберите **Управление**.
- В дереве консоли выберите **Алерты** и нажмите кнопку **Управление** на панели инструментов.
- В дереве консоли выберите **Алерты**, а затем на панели сведений щелкните правой кнопкой мыши **Параметры повторной доставки** и выберите **Управление**.
- В дереве консоли выберите **Алерты**, а затем на панели сведений дважды щелкните **Параметры повторной доставки**.

Примечание: Можно настроить различные параметры тревожных оповещений для оперативного и автономного режимов. Настройки оперативного режима (обычный профиль) применяются к клиентским компьютерам, находящимся в сети. Настройки автономного режима (офлайн-профиль) применяются к клиентским компьютерам, работающим автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Для получения дополнительной информации о политиках DeviceLock для автономного режима работы см. раздел Политики безопасности DeviceLock (офлайн-профиль).

DeviceLock создает и рассылает тревожные оповещения в момент возникновения соответствующих им событий. Если при первой попытке DeviceLock не сможет отправить оповещение, создается очередь для хранения не доставленных оповещений, которые через определенный промежуток времени высылаются повторно. Можно указать для DeviceLock максимальное количество попыток рассылки оповещений, задать интервал между попытками отправки, а также срок хранения не доставленных оповещений в очереди.

Заполните вкладку **Параметры повторной доставки** следующим образом:

- **Количество попыток повторной доставки** - Укажите максимальное количество попыток отправки оповещений, выполняемых сервисом DeviceLock, если первая попытка окончилась неудачей. Если оповещение не удалось отправить в первый раз, оно попадает в очередь и помечается как не доставленное. После каждой неудачной попытки счетчик увеличивается на единицу.

  Этот параметр должен содержать число от 0 до 999. Значение по умолчанию - `3`.

  По достижении лимита попыток сервис DeviceLock регистрирует ошибку в своем журнале аудита ("<название_канала> для алертов недоступно и временно отключено из-за ошибки: <код_ошибки> - <описание_ошибки>") и временно прекращает передачу данных по каналу рассылки оповещений (SNMP, SMTP и/или syslog).

  Сервис DeviceLock автоматически попытается восстановить соединение с указанным сервером SNMP, SMTP или syslog при проверке состояния соединения (т.е. есть ли подключение к сети или нет, подробнее см. в разделе Переключение между оперативным и автономным режимами). После восстановления соединения сервис DeviceLock возобновит рассылку оповещений.

  Для обычного и автономного профилей можно задать разные значения этого параметра.

- **Интервал повторной доставки** - Укажите, сколько времени (в секундах) сервис DeviceLock будет ждать перед повторной отправкой не доставленного оповещения. Значение должно быть в интервале от 10 до 3600 (по умолчанию `600` секунд).

- **Сохранить в очереди** - Укажите период времени (в часах), в течение которого не доставленные оповещения должны храниться в очереди до того, как будут удалены. Для всех каналов рассылки используется одна и та же очередь (SNMP, SMTP и/или syslog).

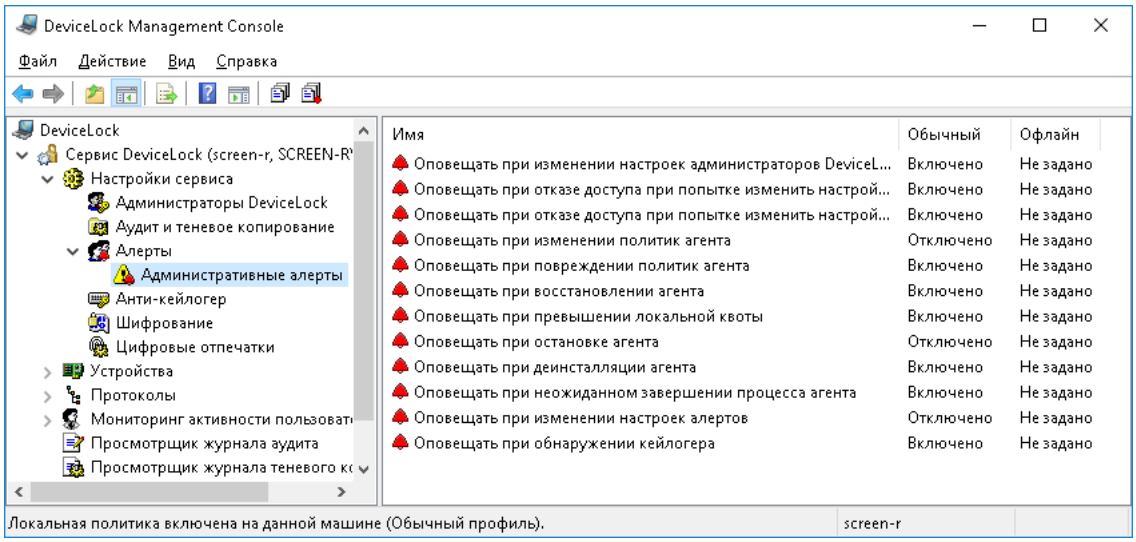
  Для этого параметра может быть установлено значение от 1 до 999 часов. Значение по умолчанию - `1` час.

  Данный параметр можно задать только для обычного профиля. Для обоих профилей (обычного и автономного) используется одно и то же значение.

Административные алерты

Административные алерты (тревожные оповещения) предназначены для оперативного информирования о критических инцидентах, требующих вмешательства администратора. После включения этой функции оповещения будут высылаться определенным адресатам при возникновении соответствующего события.

Если выбрать элемент **Административные алерты** в дереве консоли, на панели сведений отображаются административные алерты, которые можно включить или отключить.



По щелчку правой кнопкой мыши на любом алерте появляется контекстное меню, содержащее следующие команды:

- **Включить** - Включает административный алерт для оперативного (онлайн) режима.
- **Выключить** - Отключает административный алерт для оперативного (онлайн) режима.
- **Сбросить** - Сбрасывает административный алерт для оперативного (онлайн) режима в состояние "не задано". Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.
- **Включить офлайн** - Включает административный алерт для автономного режима.
- **Выключить офлайн** - Отключает административный алерт для автономного режима.
- **Сбросить офлайновые настройки** - Сбрасывает ранее заданный административный алерт для автономного режима в состояние "не задано". Если алерт для автономного режима не задан, к клиентским компьютерам, находящимся не в сети, применяется алерт, заданный для оперативного режима.
- **Управление** - Открывает диалоговое окно, в котором можно настроить сразу несколько административных алертов для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, в котором можно настроить сразу несколько административных алертов для автономного режима.
- **Удалить офлайновые настройки** - Блокирует наследование административных алертов для автономного режима и принудительно применяет административные алерты для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

Примечание: Можно настроить различные параметры административных алертов для оперативного и автономного режимов. Оперативные алерты (обычный профиль) создаются, когда клиентские компьютеры подключены к сети. Автономные алерты (офлайн-профиль) создаются, когда клиентские компьютеры работают в автономном режиме. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Для получения дополнительной информации о политиках DeviceLock для автономного режима работы, см. раздел Политики безопасности DeviceLock (офлайн-профиль).

Доступны следующие административные алерты:

- **Оповещать при изменении настроек администраторов DeviceLock** - В настройках списка администраторов сервиса DeviceLock произошли изменения. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, имя пользователя, SID пользователя и идентификатор события.
- **Оповещать при отказе доступа при попытке изменить настройки агента** - Включена безопасность DeviceLock по умолчанию, и пользователь с недостаточными правами неоднократно пытался изменить настройки сервиса DeviceLock. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, имя пользователя, SID пользователя и идентификатор события.
- **Оповещать при отказе доступа при попытке изменить настройки агента и включенной настройке 'Подавлять локальную политику'** - В DeviceLock Group Policy Manager включен параметр **Подавлять локальную политику**, и пользователь пытается изменить настройки сервиса DeviceLock при помощи консоли DeviceLock Management Console. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, имя пользователя, SID пользователя и идентификатор события.
- **Оповещать при изменении политик агента** - Один или несколько параметров сервиса DeviceLock (кроме параметров списка администраторов DeviceLock) были изменены. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип устройства или протокола, тип действий пользователя, тип профиля, имя пользователя, SID пользователя и идентификатор события.

- **Оповещать при повреждении политик агента** - Сервис DeviceLock при запуске обнаружил повреждение своих настроек. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, имя пользователя, SID пользователя и идентификатор события.

  Для проверки собственных настроек сервис DeviceLock вычисляет контрольную сумму. Все некорректные настройки автоматически исправляются.

- **Оповещать при восстановлении агента** - Удалены один или несколько установочных файлов сервиса DeviceLock. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, имя пользователя, SID пользователя и идентификатор события.

  Все удаленные файлы автоматически восстанавливаются.

- **Оповещать при превышении локальной квоты** - Превышена квота в локальном хранилище для аудита/теневого копирования данных, очереди оповещений и данных для анализа контента. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, имя пользователя, SID пользователя и идентификатор события.

  Подробную информацию о квоте в локальном хранилище см. в описании параметра Локальная квота (%).

- **Оповещать при остановке агента** - Произошел перезапуск сервиса DeviceLock. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, номер версии сервиса DeviceLock, имя пользователя, SID пользователя и идентификатор события.

- **Оповещать при деинсталляции агента** - Обнаружено, что выполняется деинсталяция сервиса DeviceLock. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, номер версии сервиса DeviceLock, имя пользователя, SID пользователя и идентификатор события.

- **Оповещать при неожиданном завершении процесса агента** - Нештатная остановка сервиса DeviceLock с последующим его перезапуском. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, номер версии сервиса DeviceLock, имя пользователя, SID пользователя и идентификатор события.

- **Оповещать при изменении настроек алертов** - Были изменены один или несколько параметров оповещений. Данный алерт рассылается согласно предыдущим настройкам оповещения. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, тип профиля, имя пользователя, SID пользователя, идентификатор процесса, связанного с событием, и идентификатор события.

- **Оповещать при обнаружении кейлогера** - Обнаружен аппаратный USB-кейлогер. Алерт содержит информацию о типе события, имя компьютера, дату и время события, тип действий пользователя, название USB-устройства, которое было определено как кейлогер, имя пользователя, SID пользователя и идентификатор события. Чтобы это уведомление приходило, следует включить параметр Протоколировать событие анти-кейлогера. За дополнительной информацией обращайтесь к разделу Анти-кейлогер данного руководства.

Управление административными алертами

Административные оповещения можно включать и выключать по отдельности или сразу.

Чтобы включить рассылку отдельных административных оповещений для оперативного режима (обычный профиль) или автономного режима (офлайн-профиль), щелкните правой кнопкой мыши любое административное оповещение и выберите **Включить** или **Включить офлайн**. Состояние административного оповещения для оперативного/автономного режима изменится с **Не задано** на **Включено**.

Включенное административное оповещение можно отключить. Для этого щелкните правой кнопкой мыши административное оповещение и выберите **Выключить** или **Выключить офлайн**. Состояние административного оповещения изменится с **Включено** на **Отключено**.

Можно также включить или отключить оповещение обычного профиля, дважды щелкнув его.

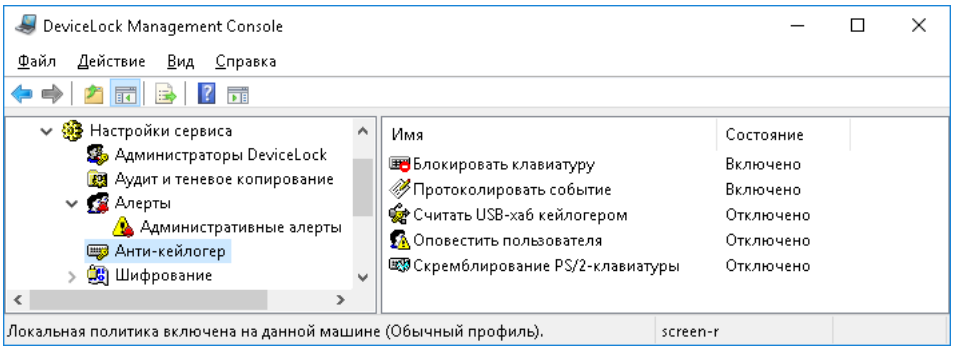
Чтобы включить рассылку множества административных оповещений обычного профиля или офлайн-профиля, щелкните правой кнопкой мыши любое административное оповещение и выберите команду **Управление** или **Управление офлайновыми настройками**. Также можно выбрать административное оповещение и нажать кнопку **Управление** или **Управление офлайновыми настройками** на панели инструментов. Затем в открывшемся диалоговом окне установите флажки рядом с административными оповещениями, которые необходимо включить. Включенные административные оповещения можно отключить. Для этого необходимо снять флажки для настроек, которые требуется отключить.

Примечание: Все флажки в диалоговом окне **Административные алерты (Офлайн)** могут иметь одно из трех состояний: установленные, снятые или в неопределенном состоянии, что соответствует состояниям **Включено**, **Отключено** и **Не задано** административных оповещений.

Анти-кейлогер

Эти настройки позволяют задать параметры обнаружения аппаратных кейлогеров (клавиатурных шпионов) и действия, которые сервис DeviceLock должен выполнить, когда кейлогер обнаружен.

Кейлогеры - это устройства, которые перехватывают и записывают в собственную память все нажатия клавиш на клавиатуре. Сервис DeviceLock обнаруживает USB-кейлогеры и блокирует клавиатуры, подсоединенные к ним. Также сервис DeviceLock может блокировать PS/2-кейлогеры.



Используйте контекстное меню, которое появляется по нажатию правой кнопки мыши на каждом параметре.

Параметры анти-кейлогера:

- Блокировать клавиатуру
- Протоколировать событие
- Считать USB-хаб кейлогером
- Оповестить пользователя
- Скремблирование PS/2-клавиатуры

Блокировать клавиатуру

Включите этот параметр, чтобы блокировать клавиатуру, подключенную к USB-кейлогеру в момент его обнаружения.

Поскольку сервис DeviceLock запускается раньше того момента, когда пользователь вводит пароль входа в Windows, блокировании клавиатуры позволит предотвратить набор пароля на клавиатуре подключенной к кейлогеру.

Примечание: Некоторые аппаратные кейлогеры продолжают записывать нажатия клавиш даже на заблокированной клавиатуре, которая не функционирует в Windows. Это происходит из-за того, что такие кейлогеры являются самодостаточными устройствами и не требуют наличия драйверов и ОС.

Протоколировать событие

Включите этот параметр, чтобы протоколировать факты обнаружения кейлогеров в журнал аудита.

Считать USB-хаб кейлогером

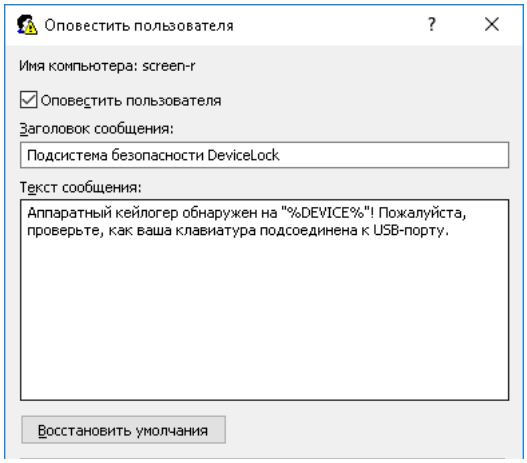
Включите этот параметр, если требуется, чтобы сервис DeviceLock считал кейлогером любой USB-хаб с подключенной к нему клавиатурой.

В противном случае сервис DeviceLock считает кейлогерами только те USB-хабы, которые занесены в его внутренний список.

Оповестить пользователя

Вы можете задать пользовательское сообщение, которое будет показываться при обнаружении аппаратных USB-кейлогеров.

Поскольку сервис DeviceLock запускается раньше того момента, когда пользователь вводит пароль входа в Windows, это сообщение может предупредить и предостеречь этого пользователя от набора пароля на клавиатуре, подключенной к кейлогеру.



Для разрешения показа этого пользовательского сообщения установите флажок **Оповестить пользователя**.

Можно задать следующие параметры:

- **Заголовок сообщения** - Текст, который будет отображаться в заголовке. В тексте заголовка допускается предопределенный макрос:
  - `%DEVICE%` - Добавляет имя клавиатуры (например, “USB-клавиатура”), полученное из системы.
- **Текст сообщения** - Основной текст сообщения. В тексте можно использовать макрос `%DEVICE%` аналогично тому, как описано выше.

Скремблирование PS/2-клавиатуры

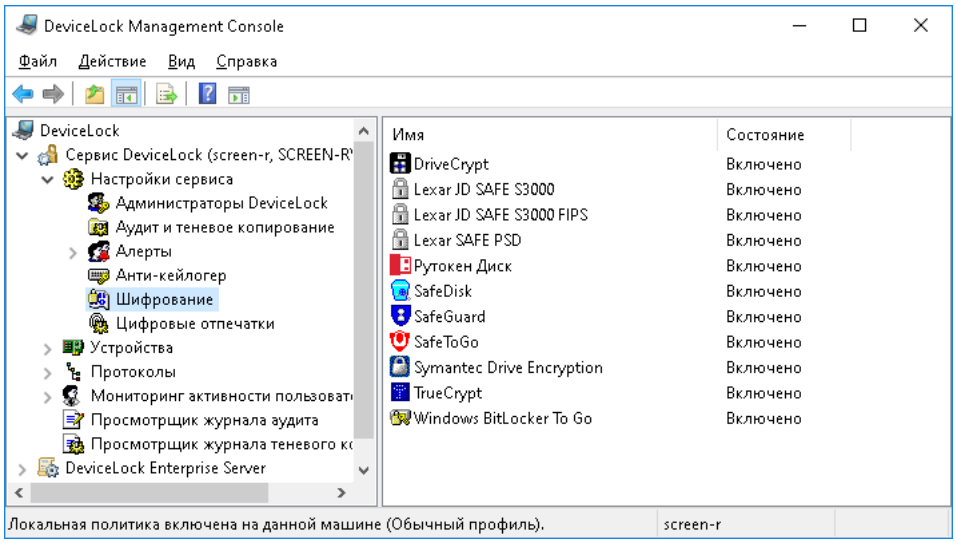
Включите этот параметр, чтобы предотвратить запись данных на PS/2-кейлогеры. Сервис DeviceLock не способен обнаруживать PS/2-кейлогеры и информировать пользователей об их возможном присутствии в системе. Однако сервис DeviceLock может искажать вводимые с PS/2-клавиатуры данные, вынуждая PS/2-кейлогеры записывать “мусор” вместо реально вводимых данных.

Примечание: Если параметр **Скремблирование PS/2-клавиатуры** включен при работе с KVM-переключателем, переключение между компьютерами с помощью клавиатуры невозможно.

Шифрование

Сервис DeviceLock может распознавать диски (USB-накопители и другие съемные устройства), на которых данные хранятся в зашифрованном виде, и применять для них так называемые "зашифрованные" разрешения (см. Группа прав "Зашифрованные"). Эта функция позволяет предотвращать запись конфиденциальных данных на носители, которые не обеспечивают их шифрование.

Список продуктов и технологий шифрования, поддерживаемых сервисом DeviceLock, появляется на панели сведений, если в дереве консоли выбрать **Сервис DeviceLock** > **Настройки сервиса** > **Шифрование**.



В списке на панели сведений приводится следующая информация:

- **Имя** - Имя продукта или технологии шифрования.
- **Состояние** - Указывает, включена ли интеграция для данного продукта или технологии:
  - **Включено** - Могут применяться "зашифрованные" разрешения.
  - **Отключено** - "Зашифрованные" разрешения не действуют.
  - **Не задано** - Параметр не задан в файле настроек сервиса DeviceLock. Это состояние возможно в редакторе настроек DeviceLock Service Settings Editor или редакторе объектов групповой политики DeviceLock Group Policy Manager.

Чтобы включить или отключить интеграцию, щелкните правой кнопкой мыши в списке на панели сведений и затем выберите команду **Включить** или **Выключить**. Чтобы установить состояние "Не задано", используйте команду **Сбросить** в редакторе настроек DeviceLock Service Settings Editor или редакторе объектов групповой политики DeviceLock Group Policy Manager.

Продукты и технологии шифрования данных

На данный момент сервис DeviceLock обеспечивает интеграцию со следующими сторонними продуктами и технологиями, используемыми для шифрования данных на съемных устройствах хранения:

- DriveCrypt
- Lexar JD SAFE S3000 и Lexar JD SAFE S3000 FIPS
- Lexar SAFE PSD
- Рутокен Диск
- SafeDisk
- SafeGuard
- SafeToGo
- Symantec Drive Encryption (бывший PGP Whole Disk Encryption)
- TrueCrypt
- Windows BitLocker To Go
- Mac OS X FileVault

Примечание: DeviceLock не поставляется вместе со сторонними продуктами шифрования и не требует их наличия для своего функционирования. Сторонний продукт шифрования должен быть правильно установлен, настроен и запущен на том же самом компьютере, где работает сервис DeviceLock, только когда требуется использовать интеграцию сервиса DeviceLock с этим сторонним продуктом.

Если не требуется, чтобы сервис DeviceLock обнаруживал диски, зашифрованные каким-либо продуктом или технологией из числа указанных выше, и применял к ним "зашифрованные" разрешения, отключите интеграцию, выполнив команду **Выключить** на соответствующем имени в списке на панели сведений консоли (см. Шифрование).

Подробнее о "зашифрованных" разрешениях см. в следующих разделах данного руководства:

Разрешения (обычный профиль)

Группа прав "Зашифрованные"

DriveCrypt

Сервис DeviceLock может обнаруживать диски, зашифрованные посредством DriveCrypt Plus Pack (DCPP), и применять к ним "зашифрованные" разрешения, когда DriveCrypt Plus Pack установлен на компьютере, где работает сервис DeviceLock с включенной интеграцией для DriveCrypt.

Подробнее о DriveCrypt Plus Pack см. на веб-сайте по адресу www.securstar.biz.

Lexar JD SAFE S3000 и Lexar JD SAFE S3000 FIPS

Сервис DeviceLock может обнаруживать USB-flash диски Lexar™ SAFE S3000 и/или SAFE S3000 FIPS и применять к ним "зашифрованные" разрешения, если у него включена интеграция для Lexar JD SAFE S3000 и/или Lexar JD SAFE S3000 FIPS, соответственно.

Подробнее о Lexar SAFE S3000 и SAFE S3000 FIPS см. в разделе "USB Flash Drive" на странице веб-сайта компании Lexar по адресу www.lexar.com/support/frequently-asked-questions.

Lexar SAFE PSD

Сервис DeviceLock может обнаруживать USB-flash диски Lexar™ SAFE PSD S1100 и применять к ним "зашифрованные" разрешения, если у него включена интеграция для Lexar SAFE PSD.

Рутокен Диск

Сервис DeviceLock может обнаруживать USB-диски, использующие технологию шифрования Рутокен, и применять к ним "зашифрованные" разрешения, если у него включена интеграция для Рутокен Диск.

О технологии Рутокен см. на сайте www.rutoken.ru.

SafeDisk

Сервис DeviceLock может обнаруживать контейнеры на USB-flash дисках и других съемных устройствах, использующих технологию шифрования SafeDisk, и применять к ним "зашифрованные" разрешения, если у него включена интеграция для SafeDisk.

Подробнее о ViPNet Safe Disk см. на веб-сайте infotecs.biz.

Примечание: Чтобы получить доступ к контейнерам SafeDisk и работать с их содержимым, пользователи должны обладать как минимум правом доступа на чтение к незашифрованным съемным устройствам.

SafeGuard

Сервис DeviceLock может обнаруживать USB-flash диски и другие съемные устройства, использующие технологию шифрования Sophos SafeGuard Easy, и применять к ним "зашифрованные" разрешения, если у него включена интеграция для SafeGuard.

Подробнее о Sophos SafeGuard Easy см. на веб-сайте компании Sophos по адресу www.sophos.com/products/safeguard-encryption.aspx.

SafeToGo

Сервис DeviceLock может обнаруживать зашифрованные USB-flash диски, использующие технологию шифрования SafeToGo™, и применять к ним "зашифрованные" разрешения, если у него включена интеграция для SafeToGo.

Подробнее о SafeToGo™ см. на веб-сайте по адресу safetogo.eu.

Symantec Drive Encryption (бывший PGP Whole Disk Encryption)

Сервис DeviceLock может обнаруживать съемные накопители, зашифрованные посредством Symantec Drive Encryption, и применять к ним "зашифрованные" разрешения, когда Symantec Drive Encryption установлен на компьютере, где работает сервис DeviceLock с включенной интеграцией для Symantec Drive Encryption.

Подробнее о Symantec Drive Encryption см. на веб-сайте компании Symantec по адресу support.symantec.com/en_US/drive-encryption.html. Инструкцию по установке и использованию PGP® Whole Disk Encryption совместно с DeviceLock см. в документе PGP/DeviceLock Integration Guide (на английском языке), подготовленном компанией PGP.

TrueCrypt

Сервис DeviceLock может обнаруживать съемные накопители, зашифрованные посредством TrueCrypt, и применять к ним "зашифрованные" разрешения, когда TrueCrypt установлен на компьютере, где работает сервис DeviceLock с включенной интеграцией для TrueCrypt.

Подробнее о TrueCrypt см. на веб-сайте по адресу www.truecrypt.org.

Примечание: Если раздел TrueCrypt создан как "File-hosted (container)", то, чтобы получить доступ к такому контейнеру и работать с его содержимым, пользователи должны обладать как минимум правом доступа на чтение к незашифрованным съемным устройствам.

Windows BitLocker To Go

Сервис DeviceLock может обнаруживать диски, использующие технологию шифрования BitLocker To Go, и применять к ним “зашифрованные” разрешения, если у него включена интеграция для Windows BitLocker To Go.

Подробнее о технологии шифрования диска BitLocker в Windows 7 и более поздних версиях Windows, см. в документации Microsoft по адресу go.microsoft.com/fwlink/?linkid=76553.

Примечание: Если интеграция с Windows BitLocker To Go включена, невозможно включить настройку групповой политики “Запретить запись на съемные диски, не защищенные BitLocker” (находится в папке “Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Шифрование диска BitLocker\Съемные носители с данными”).

Mac OS X FileVault

Сервис DeviceLock для Mac может обнаруживать диски, использующие технологию шифрования FileVault, и применять к ним “зашифрованные” разрешения, если у него включена интеграция для Mac OS X FileVault. Интеграция с FileVault не поддерживается на операционной системе Windows, так что Mac OS X FileVault отсутствует в списке узла Шифрование на панели сведений консоли, подключенной к компьютеру под управлением Windows.

Подробнее о FileVault см. в документации Apple по адресу support.apple.com/HT204837.

Узел “Устройства”

Узел **Устройства** позволяет получить доступ к следующим функциям DeviceLock:

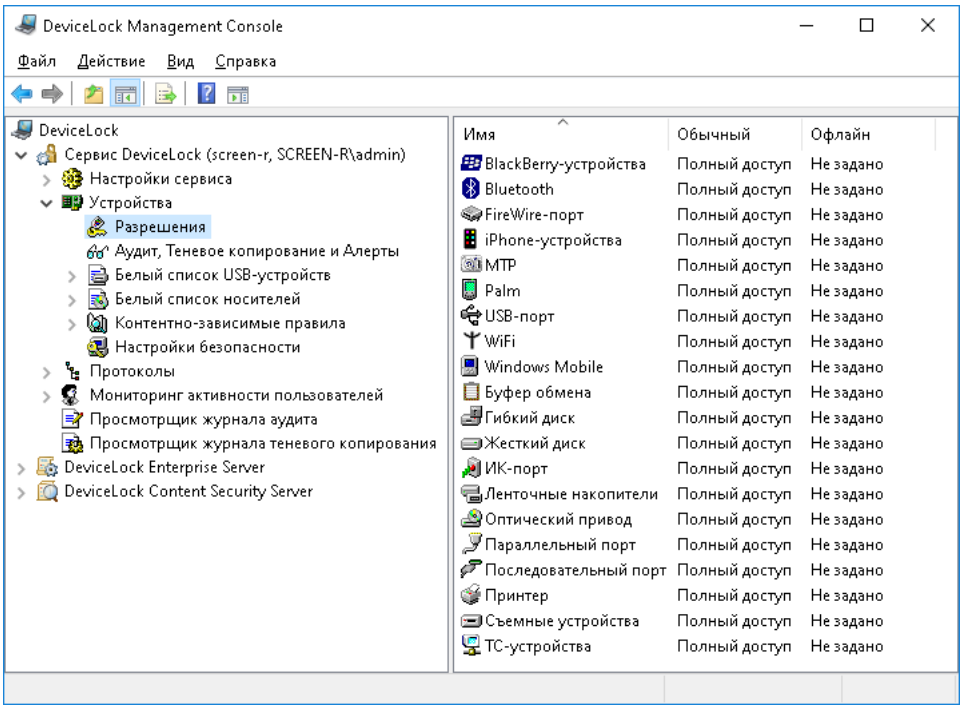
- Разрешения для устройств (см. Разрешения (обычный профиль), Управление разрешениями для автономного режима)
- Аудит, теневое копирование и алерты для устройств (см. Аудит, теневое копирование и алерты (обычный профиль), Управление правилами аудита, теневого копирования и оповещений для автономного режима)
- Белый список устройств (см. Белый список USB-устройств (обычный профиль), Управление белым списком USB-устройств для автономного режима)
- Белый список носителей (см. Белый список носителей (обычный профиль), Управление белым списком носителей для автономного режима)
- Контентно-зависимые правила для устройств (см. Правила для устройств в разделе Контентно-зависимые правила (обычный профиль), а также Управление контентно-зависимыми правилами для устройств для автономного режима)
- Настройки безопасности для устройств (см. Настройки безопасности (обычный профиль), Управление настройками безопасности для автономного режима)

Контекстное меню этого узла содержит следующую команду:

- **Сбросить политику ContentLock в неопределенное состояние** - Сбрасывает настройки ContentLock (все правила работы с контентом, кроме тех, которые основаны на типах файлов) в состояние “не задано”.

Разрешения (обычный профиль)

В узле **Разрешения** перечисляются типы устройств, для которых можно установить разрешения.



Примечание: При установке разрешений на тип устройств они устанавливаются для всех устройств данного типа. Невозможно установить разные разрешения на устройства одного типа, например, на два съемных USB-диска. Чтобы задать разные права доступа к USB-устройствам одного типа, можно воспользоваться белым списком устройств (см. Белый список USB-устройств (обычный профиль)).

Поддерживается контроль двух типов - на уровне интерфейса (порта) и на уровне типа. Некоторые устройства проверяются на обоих уровнях, в то время как другие - только на одном.

Дополнительные сведения о том, как работает контроль доступа к устройствам в DeviceLock, можно найти в разделе Управляемый контроль доступа данного руководства.

DeviceLock поддерживает следующие типы устройств:

- **BlackBerry-устройства** (уровень типа) - Устройства BlackBerry с любым интерфейсом подключения к компьютеру (USB, Bluetooth).
- **Bluetooth** (уровень типа) - Внешние и внутренние Bluetooth-адаптеры с любым интерфейсом подключения к компьютеру (USB, PCMCIA и т.д.).
- **Буфер обмена** - Буфер обмена Windows. DeviceLock контролирует операции копирования/вставки данных из буфера обмена.

  Внимание: Сразу после установки сервиса DeviceLock пользователь может копировать и вставлять данные между приложениями, даже если настроен запрет на доступ к буферу обмена. В этом случае необходимо перезагрузить компьютер, чтобы настройки доступа к буферу обмена вступили в силу.

- **FireWire-порт** (уровень интерфейса) - Устройства, которые могут быть подключены к FireWire-порту (IEEE 1394), за исключением хабов.

- **Гибкий диск** (уровень типа) - Внешние и внутренние дисководы с любым интерфейсом подключения к компьютеру (IDE, USB, PCMCIA и т.д.). Существуют некоторые модели нестандартных дисководов, которые распознаются Windows как сменные накопители, в этом случае DeviceLock также относит такие дисководы к типу **Съемные устройства**.
- **Жесткий диск** (уровень типа) - Внешние и внутренние жесткие диски с любым интерфейсом подключения к компьютеру (IDE, SATA, SCSI и т.д.). DeviceLock относит все жесткие диски, подключаемые через интерфейсы USB, FireWire и PCMCIA к типу **Съемные устройства**. Также DeviceLock относит к типу **Съемные устройства** некоторые жесткие диски (обычно с интерфейсом подключения SATA и SCSI), если они поддерживают функцию "горячего" подключения и при этом на них не установлена используемая ОС Windows.

  Примечание: Даже если вы полностью запретили доступ к жесткому диску, пользователи с правами локального администратора и учетная запись СИСТЕМА смогут получить доступ к разделу этого диска, на котором установлена текущая ОС Windows.

- **ИК-порт** (уровень интерфейса) - Устройства, которые могут быть подключены к компьютеру через инфракрасный порт (IrDA).
- **iPhone-устройства** (уровень типа) - Устройства iPhone, iPod Touch и iPad. DeviceLock контролирует те iPhone, iPod Touch и iPad устройства, которые работают с компьютером через приложение iTunes или его программный интерфейс (API).
- **MTP** (уровень типа) - Устройства (телефоны на базе Android и т.д.), которые работают с компьютером через Media Transfer Protocol (MTP). DeviceLock контролирует устройства с любым интерфейсом подключения к компьютеру (USB, IP, Bluetooth).
- **Оптический привод** (уровень типа) - Внешние и внутренние CD/DVD/BD-приводы (включая пишущие) с любым интерфейсом подключения к компьютеру (IDE, SATA, USB, FireWire, PCMCIA и т.д.).
- **Palm** (уровень типа) - Устройства, работающие под управлением ОС Palm OS с любым интерфейсом подключения к компьютеру (USB, COM, IrDA, Bluetooth, WiFi). DeviceLock контролирует те Palm-устройства, которые работают с компьютером через приложение HotSync.
- **Параллельный порт** (уровень интерфейса) - Устройства, которые могут быть подключены к компьютеру через параллельный порт (LPT).
- **Принтер** (уровень типа) - Локальные и сетевые принтеры с любым интерфейсом подключения к компьютеру (USB, LPT, Bluetooth и т.д.). DeviceLock может также контролировать виртуальные принтеры, т.е. принтеры, которые печатают не на реальном физическом устройстве, а, например, перенаправляют печать в файл.
- **Съемные устройства** (уровень типа) - Устройства с любым интерфейсом подключения к компьютеру (USB, FireWire, PCMCIA, IDE, SATA, SCSI и т.д.), которые распознаются Windows как сменные накопители (например, USB-флешки, карт-ридеры, магнитооптические приводы и т.п.). DeviceLock относит все жесткие диски, подключаемые через интерфейсы USB, FireWire и PCMCIA к типу **Съемные устройства**. Также DeviceLock относит к типу **Съемные устройства** некоторые жесткие диски (обычно с интерфейсом подключения SATA и SCSI), если они поддерживают функцию "горячего" подключения и при этом на них не установлена используемая ОС Windows.
- **Последовательный порт** (уровень интерфейса) - Устройства, которые могут быть подключены к компьютеру через последовательный порт (COM), включая внутренние модемы.
- **Ленточные накопители** (уровень типа) - Внешние и внутренние ленточные накопители с любым интерфейсом подключения к компьютеру (SCSI, USB, IDE и т.д.).

- **TC-устройства** (уровень интерфейса) - Подключенные диски (жесткие, съемные и оптические диски), последовательные порты, USB-устройства и буфер обмена, перенаправленные с удаленного терминала в опубликованное приложение или виртуальный рабочий стол, запущенные на серверной стороне терминальной сессии. DeviceLock контролирует перенаправление устройств, портов и буфера обмена, поддерживаемых протоколами Microsoft RDP, Citrix ICA, VMware PCoIP и HTML5/WebSockets в средах виртуализации Microsoft RDS, Citrix XenDesktop, Citrix XenApp, Citrix XenServer и VMware View.

  Кроме того, DeviceLock контролирует операции обмена данными между буферами обмена (Windows Clipboard) гостевой операционной системы, работающей в среде виртуализации VMware Workstation, VMware Player, Oracle VM VirtualBox или Windows Virtual PC, и операционной системой хоста.

- **USB-порт** (уровень интерфейса) - Устройства, которые могут быть подключены к USB-порту, за исключением хабов.

- **WiFi** (уровень типа) - Внешние и внутренние WiFi-адаптеры с любым интерфейсом подключения к компьютеру (USB, PCMCIA и т.д.).

  Примечание: Используя тип WiFi, вы можете контролировать доступ пользователей к самим устройствам этого типа, но не к сетям.

- **Windows Mobile** (уровень типа) - Устройства, работающие под управлением ОС Windows Mobile с любым интерфейсом подключения к компьютеру (USB, COM, IrDA, Bluetooth, WiFi). DeviceLock контролирует те Windows Mobile-устройства, которые работают с компьютером через приложения Windows Mobile Device Center (WMDC) и Microsoft ActiveSync или их программный интерфейс (API).

Установка разрешений

Чтобы установить разрешения на тип устройства, выделите его (для одновременного выделения нескольких типов устройств используйте клавиши Ctrl и/или Shift) и выберите команду **Установить разрешения** или **Установить офлайновые разрешения** из контекстного меню, либо нажмите соответствующую кнопку на панели инструментов.

Примечание: Можно установить различные разрешения для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Разрешения для оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Разрешения для автономного режима (офлайн-профиль) применяются, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Описание политик DeviceLock для автономного режима можно найти в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по установке разрешений см. в разделе Управление разрешениями для автономного режима.

Если в DeviceLock Group Policy Manager или DeviceLock Service Settings Editor нужно сбросить разрешения для оперативного режима в состояние “не задано”, выберите команду **Сбросить** из контекстного меню.

Чтобы сбросить разрешения, заданные для автономного режима, в состояние “не задано”, выберите команду **Сбросить офлайновые настройки** из контекстного меню. Если разрешения для автономного режима не заданы, к клиентским компьютерам, находящимся не в сети, применяются разрешения, заданные для оперативного режима.

Если в DeviceLock Group Policy Manager или DeviceLock Service Settings Editor требуется заблокировать наследование разрешений, заданных для автономного режима, чтобы затем принудительно применить разрешения, заданные для оперативного режима, выберите команду **Удалить офлайновые настройки** из контекстного меню.

Разрешения для оперативного режима могут иметь одно из следующих состояний:

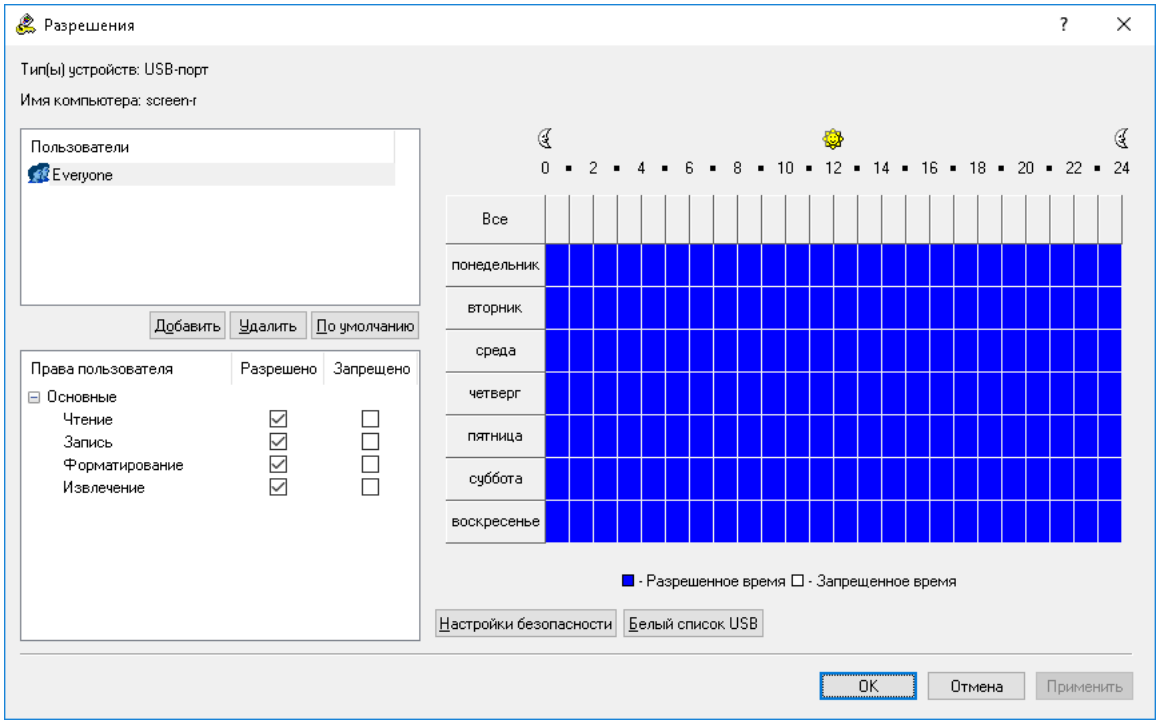
- **Задано** - Разным учетным записям назначены разные разрешения для устройств данного типа.
- **Полный доступ** - У всех учетных записей есть полный доступ к устройствам данного типа.

  Это состояние отображается, например, когда разрешения заданы только для учетной записи “Все” (Everyone) таким образом, что у нее есть полный доступ к устройствам.
- **Нет доступа** - Нет учетных записей, имеющих доступ к устройствам данного типа.

  Это состояние отображается, например, когда учетной записи “Все” (Everyone) явно запрещен любой доступ к устройствам данного типа или разрешения не заданы ни для каких учетных записей. Обратите внимание, что запрет для учетной записи “Все” (Everyone) отменяет все разрешения для других учетных записей.
- **Не задано** - Настройки разрешений для данного протокола не заданы.

Диалоговое окно “Разрешения”

Чтобы установить разрешения на тип устройства для оперативного режима, выделите его (для одновременного выделения нескольких типов устройств используйте клавиши Ctrl и/или Shift) и выберите пункт **Установить разрешения** из контекстного меню, либо нажмите соответствующую кнопку на панели инструментов.



Имена пользователей и групп пользователей, назначенных данному типу, отображаются в списке учетных записей в левой верхней части диалогового олкна **Разрешения**.

Чтобы добавить нового пользователя или группу пользователей в список учетных записей, нажмите кнопку **Добавить**. Вы можете добавить несколько учетных записей одновременно.

Для удаления учетных записей из списка используйте кнопку **Удалить**. Для одновременного удаления нескольких записей используйте клавиши Ctrl и/или Shift.

Чтобы установить для устройства разрешения по умолчанию, нажмите кнопку **По умолчанию**. Перечень таких разрешений см. в разделе Разрешения по умолчанию.

Используя контроль по времени, можно задать период, когда выбранный пользователь или группа будут иметь (или не иметь) доступ к устройствам. Специальный элемент управления для выбора времени расположен в правом верхнем углу диалога **Разрешения**. Используйте левую кнопку мыши для выбора разрешенного времени. Для выбора времени, когда доступ запрещен, используйте правую кнопку мыши. Для задания разрешенных или запрещенных периодов вы также можете использовать клавиатуру: стрелки для навигации и пробел для переключения между разрешенным/запрещенным временем.

Чтобы указать действия пользователя, которые должны быть разрешены или запрещены, установите соответствующие права доступа. Предусмотрены три группы прав доступа:

- **Основные** - Применяются к большинству устройств, за исключением шифрованных. Подробнее см. в разделе Группа прав “Основные”.
- **Зашифрованные** - Применяются к устройствам, которые DeviceLock распознает как шифрованные. Подробнее см. в разделе Группа прав “Зашифрованные”.
- **Специальные разрешения** - Применяются только к следующим типам устройств: iPhone-устройства, Windows Mobile, Palm и Буфер обмена. Подробнее см. в разделе Группа прав “Специальные разрешения”.

Если у некоторой учетной записи установлен флаг **Разрешено** для всех прав, это означает, что данная учетная запись имеет полный доступ. Если у некоторой учетной записи установлен флаг **Запрещено** для всех прав, это означает, что для данной учетной записи любой доступ запрещен. Если у некоторой учетной записи флаги **Разрешено** и **Запрещено** сняты для всех прав, это означает, что данная учетная запись наследует права доступа из своей пользовательской группы (если такая группа отсутствует, то для такой учетной записи любой доступ запрещен).

Примечание: Право "любой доступ запрещен" имеет приоритет над всеми остальными правами. Это означает, что если группе, к которой принадлежит пользователь, назначить право "любой доступ запрещен", а самому пользователю дать полный доступ, то пользователь все равно не получит доступа к устройству. Если требуется запретить доступ для какого-либо пользователя (или группы), просто удалите его из списка учетных записей, вместо того, чтобы устанавливать для него право "любой доступ запрещен".

Кроме того, учетная запись **Все** (Everyone) имеет приоритет над всеми остальными учетными записями. Это означает, что если учетной записи **Все** установлено право "любой доступ запрещен", то никто вообще не сможет получить доступ к устройству. Появится следующее сообщение: "Вы запретили для всех доступ к типу(ам) устройств: <список типов устройств>. Никто не сможет получить доступ к типу(ам) устройств: <список типов устройств>. Продолжить?"

Даже если вы полностью запретили доступ к жесткому диску, члены локальной группы "Администраторы" и учетная запись СИСТЕМА смогут получить доступ к разделу этого диска, на котором установлена используемая ОС Windows.

Мы рекомендуем добавлять в список учетных записей только тех пользователей, которые должны иметь доступ к устройству. Если список учетных записей пуст, это означает, что никто не имеет доступ к устройству. Также настоятельно рекомендуется добавить учетную запись СИСТЕМА с правом полного доступа к жестким дискам и оптическим приводам.

На некоторых компьютерах пользователи могут видеть следующее сообщение при входе в систему: "Не удалось настроить устройство Компакт-дисковод. Подробнее в журнале событий." Это значит, что учетная запись СИСТЕМА не может получить доступ к CD/DVD/BD-приводу. Чтобы избежать такой ситуации, установите право полного доступа к оптическому приводу для учетной записи СИСТЕМА.

Группа прав "Основные"

Права из группы **Основные** применяются к большинству типов устройств. Эти права не влияют на доступ к устройствам, которые DeviceLock распознает как шифрованные (список таких устройств см. в разделе Шифрование). Предусмотрены следующие основные права доступа:

- **Чтение** - Разрешает чтение данных с устройства. Данное право применимо ко всем типам, кроме типов Буфер обмена и Принтер.
- **Запись** - Разрешает запись данных на устройство. Для всех типов, кроме Windows Mobile, это право можно установить, только если установлено право Чтение из группы Основные. Данное право не может быть отключено для следующих типов: BlackBerry-устройства, Bluetooth, ИК-порт, Параллельный порт, Последовательный порт и WiFi. Если право Запись запрещено для типов USB-порт и FireWire-порт, то на устройствах хранения, таких как флэш-накопители, дисководы, жесткие и оптические диски, можно читать информацию, но не записывать, а все прочие устройства (USB-принтеры, сканеры и т. д.) недоступны.
- **Форматирование** - Разрешает форматирование и другие действия, для которых необходим прямой доступ к устройству. Это право можно установить, только если установлено право Чтение из группы Основные. Данное право применимо только к следующим типам: FireWire-порт, Гибкий диск, Жесткий диск, Съемные устройства и USB-порт. Если это право установлено для типов USB-порт и FireWire-порт, то оно влияет только на устройства хранения данных, подключаемые к этим портам.

- **Извлечение** - Разрешает извлечение сменного носителя из устройства. Вы можете установить это право только в том случае, если установлено право Чтение из группы Основные. Это право контролирует только программное извлечение носителя. Физическое извлечение путем нажатия кнопки на передней панели устройства не может быть предотвращено. Данное право применимо только к следующим типам: FireWire-порт, Гибкий диск, Оптический привод, Съемные устройства и USB-порт. Если это право установлено для типов USB-порт и FireWire-порт, то оно влияет только на устройства хранения данных, подключаемые к этим портам.
- **Выполнение** - Разрешает удаленное выполнение кода на стороне устройства. Данное право применимо только к типу Windows Mobile.
- **Модем** - Разрешает использование функции Internet Tethering. Применимо к типу iPhone-устройства.
- **Печать** - Разрешает печать документов. Данное право применимо только к типу Принтер.
- **Копирование в буфер обмена** - Разрешает вставку данных из буфера обмена. Данное право применимо только к типу Буфер обмена. Это право автоматически предоставляет полный доступ к буферу обмена.
- **Чтение с подключенного диска** - Разрешает чтение данных с подключенных дисков в терминальной сессии. Применимо только к типу ТС-устройства.
- **Запись на подключенный диск** - Разрешает запись данных на подключенные диски в терминальной сессии. Применимо только к типу ТС-устройства.
- **Доступ к последовательному порту** - Разрешает доступ к последовательным портам во время терминальной сессии. Применимо только к типу ТС-устройства.
- **Доступ к USB-устройствам** - Разрешает доступ к USB-устройствам во время терминальной сессии. Применимо только к типу ТС-устройства.
- **Буфер обмена входящий текст** - Разрешает вставку текстовых данных из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.
- **Буфер обмена исходящий текст** - Разрешает вставку текстовых данных из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.
- **Буфер обмена входящие изображения** - Разрешает вставку графических данных из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.
- **Буфер обмена исходящие изображения** - Разрешает вставку графических данных из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.
- **Буфер обмена входящие аудио данные** - Разрешает вставку аудиоданных из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.
- **Буфер обмена исходящие аудио данные** - Разрешает вставку аудиоданных из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.
- **Буфер обмена входящие файлы** - Разрешает вставку файлов из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.
- **Буфер обмена исходящие файлы** - Разрешает вставку файлов из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.

- **Буфер обмена входящие неизвестные данные** - Разрешает вставку всех прочих данных из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.
- **Буфер обмена исходящие неизвестные данные** - Разрешает вставку всех прочих данных из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу ТС-устройства.

Группа прав "Зашифрованные"

Права из группы **Зашифрованные** применяются к устройствам, которые DeviceLock распознает как шифрованные (подробнее см. в разделе Шифрование). Предусмотрены следующие права доступа к шифрованным устройствам:

- **Чтение** - Разрешает чтение данных с шифрованного устройства. Применимо к типу Съемные устройства.
- **Запись** - Разрешает запись данных на шифрованное устройство. Это право можно установить, только если установлено право **Чтение** из группы **Зашифрованные**. Применимо к типу Съемные устройства.
- **Форматирование** - Разрешает форматирование и другие действия, для которых необходим прямой доступ к шифрованному устройству. Это право можно установить, только если установлено право **Чтение** из группы **Зашифрованные**. Применимо к типу Съемные устройства.

Группа прав "Специальные разрешения"

Права из группы **Специальные разрешения** применяются только к следующим типам устройств: iPhone-устройства, Windows Mobile, Palm и Буфер обмена. Типы данных ("Календарь", "Контакты", "Задачи", и т.д.), которые контролируются данными правами для типов iPhone-устройства, Windows Mobile и Palm, представляют те же типы данных, что и их аналоги в приложениях iTunes, HotSync, Microsoft ActiveSync и WMDC. Для типа Palm можно включить любое право на запись, только если включено соответствующее ему право на чтение. Предусмотрены следующие специальные разрешения:

- **Чтение календаря** - Разрешает чтение данных календаря с мобильного устройства.
- **Запись календаря** - Разрешает запись данных календаря на мобильное устройство.
- **Чтение контакта** - Разрешает чтение контактов с мобильного устройства.
- **Запись контакта** - Разрешает запись контактов на мобильное устройство.
- **Чтение электронной почты** - Разрешает чтение электронной почты с мобильного устройства. Для типа iPhone-устройства этот тип данных представляет настройки учетной записи электронной почты, но не сообщения, так как приложение iTunes не поддерживает синхронизацию сообщений.
- **Запись электронной почты** - Разрешает запись электронной почты на мобильное устройство. Для типа iPhone-устройства этот тип данных представляет настройки учетной записи электронной почты, но не сообщения, так как приложение iTunes не поддерживает синхронизацию сообщений.
- **Чтение вложения** - Разрешает чтение вложений электронной почты с устройств типа Windows Mobile. Это право можно установить, только если установлено право **Чтение электронной почты** из группы **Специальные разрешения**.
- **Запись вложения** - Разрешает запись вложений электронной почты на устройства типа Windows Mobile. Это право можно установить, только если установлено право **Запись электронной почты** из группы **Специальные разрешения**.
- **Чтение избранного** - Разрешает чтение избранного (закладок) с мобильных устройств. Применимо к типам Windows Mobile и iPhone-устройства.
- **Запись избранного** - Разрешает запись избранного (закладок) на мобильные устройства. Применимо к типам Windows Mobile или iPhone-устройства.

- **Чтение файла** - Разрешает чтение файлов с мобильного устройства. Для типа iPhone-устройства в качестве файлов рассматриваются потоки данных Приложения в iTunes.
- **Запись файла** - Разрешает запись файлов на мобильное устройство. Для типа Palm данное право также включает право **Запись документа** из группы **Специальные разрешения**. Для типа iPhone-устройства в качестве файлов рассматриваются потоки данных Приложения в iTunes.
- **Чтение медиа-данных** - Разрешает чтение медиа-данных с устройств типа Windows Mobile при помощи Windows Media Player и чтение медиа-файлов с устройств типа Palm или iPhone-устройства. Это право можно установить, только если установлено право **Чтение файла** из группы **Специальные разрешения**. Для типа Windows Mobile это право также требует права **Выполнение** из группы **Основные**. Для типа iPhone-устройства медиа-данные включают в себя следующие типы данных iTunes: "Рингтоны", "Музыка", "Аудиокниги", "Фото", "Подкасты" (аудио- и видеоподкасты), "Фильмы", "Телешоу", "Фильмы, взятые напрокат".
- **Запись медиа-данных** - Разрешает запись медиа-данных на устройства типа Windows Mobile при помощи Windows Media Player и запись медиа-файлов на устройства типа Palm или iPhone-устройства. Это право можно установить, только если установлено право **Запись файла** из группы **Специальные разрешения**. Для типа Windows Mobile это право также требует права **Выполнение** из группы **Основные**. Для типа iPhone-устройства медиа-данные включают в себя следующие типы данных iTunes: "Рингтоны", "Музыка", "Аудиокниги", "Фото", "Подкасты" (аудио- и видеоподкасты), "Фильмы", "Телешоу", "Фильмы, взятые напрокат".
- **Чтение бэкапа** - Разрешает создание резервной копии устройств типа iPhone-устройства посредством чтения данных с устройства.

  Примечание: Программа iTunes создает резервные копии iPhone-устройства каждый раз, когда выполняется синхронизация с iTunes (автоматически при первой синхронизации и при каждом подключении к компьютеру). Чтобы синхронизация проходила успешно, необходимо предоставить пользователям право Чтение бэкапа для типа iPhone-устройства. В противном случае, если программа iTunes будет автоматически создавать резервные копии iPhone-устройства, сеанс синхронизации будет прерываться.

  Чтобы избежать прерывания сеанса синхронизации, необходимо настроить программу iTunes для синхронизации только тех данных, к которым разрешен доступ.

- **Запись бэкапа** - Разрешает восстановление устройств типа iPhone-устройства посредством записи резервной копии данных на устройство.
- **Чтение заметки** - Разрешает чтение заметок с мобильного устройства. Для типа Palm это право контролирует типы данных "Memos" и "Note Pad".
- **Чтение заметки** - Разрешает запись заметок на мобильное устройство. Для типа Palm это право контролирует типы данных "Memos" и "Note Pad".
- **Чтение БД Pocket Access** - Разрешает чтение баз данных Pocket Access с устройств типа Windows Mobile.
- **Запись БД Pocket Access** - Разрешает запись баз данных Pocket Access на устройства типа Windows Mobile.
- **Чтение задачи** - Разрешает чтение задач с мобильного устройства.
- **Запись задачи** - Разрешает запись задач на мобильное устройство.
- **Чтение расхода** - Разрешает чтение данных приложения Palm Expense с устройств типа Palm.
- **Запись расхода** - Разрешает запись данных приложения Palm Expense на устройства типа Palm.
- **Чтение документа** - Разрешает чтение документов с устройств типа Palm. Это право можно установить, только если установлено право **Запись файла** из группы **Специальные разрешения**.

- **Запись документа** - Разрешает запись документов на устройства типа Palm. Это право можно установить, только если установлено право **Запись файла** из группы **Специальные разрешения**.
- **Чтение неидентифицированного содержимого** - Разрешает чтение некатегоризированных данных с устройств типа Windows Mobile.
- **Запись неидентифицированного содержимого** - Разрешает запись некатегоризированных данных на устройства типа Windows Mobile.
- **Копирование текста** - Разрешает вставку текстовых данных из буфера обмена.
- **Копирование изображения** - Разрешает вставку графических данных из буфера обмена.
- **Копирование аудио данных** - Разрешает вставку аудио данных из буфера обмена.
- **Копирование файла** - Разрешает вставку файлов из буфера обмена.
- **Копирование неидентифицированного содержимого** - Разрешает вставку некатегоризированных данных из буфера обмена.
- **Копирование экрана** - Разрешает создание снимков экрана (снимков всего экрана, активного окна или любой части экрана).

Примечание: Снимки экрана, сделанные при помощи специальных программ для создания снимков экрана, сохраняются напрямую в файлы, в то время как снимки экрана, сделанные с помощью клавиши PRINT SCREEN, сначала копируются в буфер обмена, а затем вставляются в нужную программу (например, Microsoft Word или Paint). При использовании специальных программ событие снимков экрана попадает в аудит сразу при создании снимка экрана такой программой, а при нажатии клавиши PRINT SCREEN, событие попадает в аудит только при вставке в нужную программу.

Чтобы делать снимки экрана с помощью клавиши PRINT SCREEN, пользователю нужны права **Копирование изображения** и **Копирование экрана**. Если у пользователей нет права **Копирование экрана**, они не могут делать снимки экрана ни с помощью клавиши PRINT SCREEN, ни с помощью специальных программ для создания снимков экрана.

При настройке специальных разрешений необходимо учитывать следующее:

- Права **Копирование текста**, **Копирование изображения**, **Копирование аудио данных**, **Копирование файла** и **Копирование неидентифицированного содержимого** не контролируют копирование данных в буфер обмена. Пользователи всегда могут копировать данные в буфер обмена, вне зависимости от предоставленных им прав.
- В некоторых случаях пользователи могут использовать буфер обмена для переноса по отдельности или в различных комбинациях разных типов данных в формате RTF (таких как Текст, Изображение, Файл). Чтобы разрешить пользователям копировать и вставлять различные типы данных в формате RTF, им необходимо предоставить соответствующие права (такие как **Копирование текста**, **Копирование изображения** и **Копирование файла**).
- Если доступ (для чтения и/или записи) к какому-нибудь типу данных запрещен в процессе синхронизации устройств типа iPhone-устройства или Windows Mobile, необходимо заново подключить устройство для продолжения его использования.
- При попытке синхронизировать устройство типа Palm по сети сеанс синхронизации прерывается, если доступ к какому-нибудь типу данных запрещен DeviceLock. Чтобы избежать такой ситуации, необходимо до начала синхронизации настроить приложение HotSync для синхронизации только тех данных, к которым разрешен доступ.

Разрешения по умолчанию

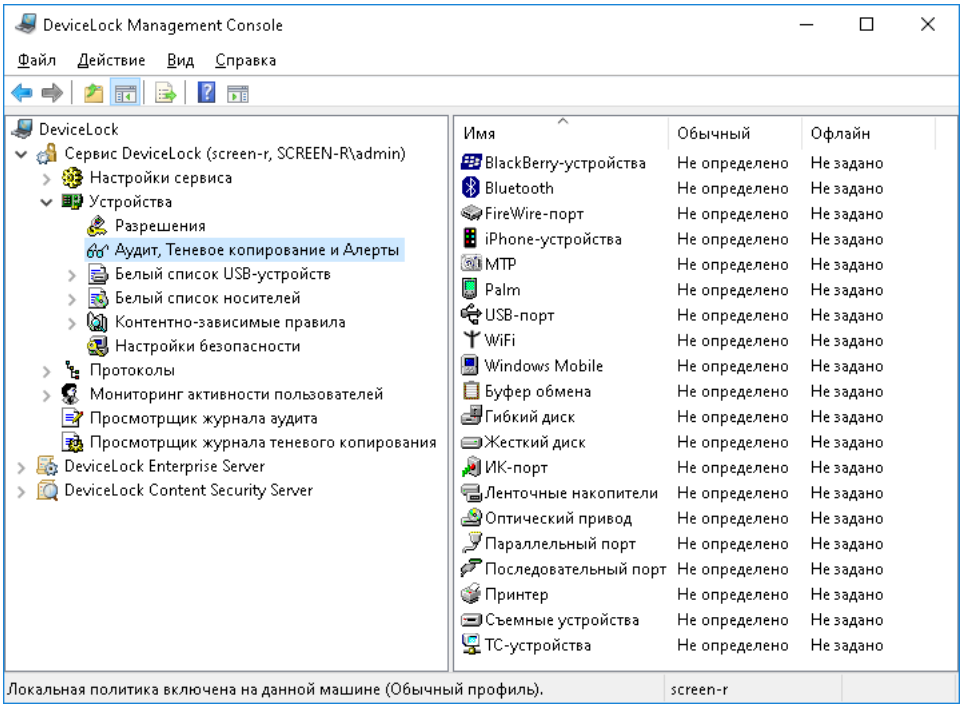
В диалоговом окне **Разрешения** предоставляется возможность установить разрешения по умолчанию для доступа к устройствам. Эти разрешения назначаются группам Все (Everyone) и Администраторы (Administrators), а также учетной записи СИСТЕМА (SYSTEM). В следующей таблице перечислены разрешения по умолчанию для каждого типа устройств.

Учетная запись/ Тип устройств	**Все**	**Администраторы**	**СИСТЕМА**
BlackBerry-устройства	Основные: Чтение, Запись	Основные: Чтение, Запись	Основные: Чтение, Запись
Bluetooth	Основные: Чтение, Запись	Основные: Чтение, Запись	Основные: Чтение, Запись
Буфер обмена	Основные: Копирование в буфер обмена Специальные разрешения: Копирование текста, Копирование изображения, Копирование аудио данных, Копирование файла, Копирование экрана, Копирование неидентифицированного содержимого	Основные: Копирование в буфер обмена Специальные разрешения: Копирование текста, Копирование изображения, Копирование аудио данных, Копирование файла, Копирование экрана, Копирование неидентифицированного содержимого	Основные: Копирование в буфер обмена Специальные разрешения: Копирование текста, Копирование изображения, Копирование аудио данных, Копирование файла, Копирование экрана, Копирование неидентифицированного содержимого
FireWire-порт	Основные: Чтение, Запись, Извлечение	Основные: Чтение, Запись, Форматирование, Извлечение	Основные: Чтение, Запись, Форматирование, Извлечение
Гибкий диск	Основные: Чтение, Запись, Извлечение	Основные: Чтение, Запись, Форматирование, Извлечение	Основные: Чтение, Запись, Форматирование, Извлечение
Жесткий диск	Основные: Чтение, Запись	Основные: Чтение, Запись, Форматирование	Основные: Чтение, Запись, Форматирование
ИК-порт	Основные: Чтение, Запись	Основные: Чтение, Запись	Основные: Чтение, Запись
iPhone-устройства	Основные: Чтение, Запись, Модем	Основные: Чтение, Запись, Модем	Основные: Чтение, Запись, Модем
MTP	Основные: Чтение, Запись	Основные: Чтение, Запись	Основные: Чтение, Запись
Palm	Основные: Чтение, Запись	Основные: Чтение, Запись	Основные: Чтение, Запись
Параллельный порт	Основные: Чтение, Запись	Основные: Чтение, Запись	Основные: Чтение, Запись
Принтер	Основные: Печать	Основные: Печать	Основные: Печать

Учетная запись/ Тип устройств	Все	Администраторы	СИСТЕМА
Съемные устройства	Основные: Чтение, Запись, Извлечение Зашифрованные: Чтение, Запись, Форматирование	Основные: Чтение, Запись, Форматирование, Извлечение Зашифрованные: Чтение, Запись, Форматирование	Основные: Чтение, Запись, Форматирование, Извлечение Зашифрованные: Чтение, Запись, Форматирование
Последовательный порт	Основные: Чтение, Запись	Основные: Чтение, Запись	Основные: Чтение, Запись
Ленточные накопители	Основные: Чтение, Запись, Извлечение	Основные: Чтение, Запись, Форматирование, Извлечение	Основные: Чтение, Запись, Форматирование, Извлечение
ТС-устройства	Основные: Чтение с подключенного диска, Доступ к последовательному порту, Доступ к USB-устройствам, Буфер обмена входящий текст, Буфер обмена входящие изображения, Буфер обмена входящие аудио данные, Буфер обмена входящие файлы, Буфер обмена входящие неизвестные данные	Основные: Чтение с подключенного диска, Запись на подключенный диск, Доступ к последовательному порту, Доступ к USB-устройствам, Буфер обмена входящий текст, Буфер обмена исходящий текст, Буфер обмена входящие изображения, Буфер обмена исходящие изображения, Буфер обмена входящие аудио данные, Буфер обмена исходящие аудио данные, Буфер обмена входящие файлы, Буфер обмена исходящие файлы, Буфер обмена входящие неизвестные данные, Буфер обмена исходящие неизвестные данные	Основные: Чтение с подключенного диска, Запись на подключенный диск, Доступ к последовательному порту, Доступ к USB-устройствам, Буфер обмена входящий текст, Буфер обмена исходящий текст, Буфер обмена входящие изображения, Буфер обмена исходящие изображения, Буфер обмена входящие аудио данные, Буфер обмена исходящие аудио данные, Буфер обмена входящие файлы, Буфер обмена исходящие файлы, Буфер обмена входящие неизвестные данные, Буфер обмена исходящие неизвестные данные
USB-порт	Основные: Чтение, Запись, Извлечение	Основные: Чтение, Запись, Форматирование, Извлечение	Основные: Чтение, Запись, Форматирование, Извлечение
WiFi	Основные: Чтение, Запись	Основные: Чтение, Запись	Основные: Чтение, Запись
Windows Mobile	Основные: Чтение, Запись, Выполнение	Основные: Чтение, Запись, Выполнение	Основные: Чтение, Запись, Выполнение

Аудит, теневое копирование и алерты (обычный профиль)

В узле **Аудит, Теневое копирование и Алерты** перечислены типы устройств, для которых можно настроить правила аудита, теневого копирования и тревожные оповещения (алерты).



Настройка разрешений, правил аудита, теневого копирования и алертов выполняется примерно одинаково, поэтому ознакомьтесь сначала с разделом Разрешения (обычный профиль) данного руководства.

Сервис DeviceLock может использовать стандартную подсистему ведения протоколов событий (журнал событий Windows) для регистрации информации об устройствах. Это особенно важно для системных администраторов, поскольку они могут использовать любое программное обеспечение для просмотра стандартных журналов Windows. Например, можно использовать стандартную программу **Просмотр событий**. Также сервис DeviceLock может использовать собственный защищенный журнал. Данные из этого журнала передаются на сервер DeviceLock Enterprise Server для централизованного хранения в базе данных. Возможно также передавать данные на сервер syslog. Место и способ хранения данных аудита определяется параметром Тип журнала аудита из раздела Настройки сервиса.

Консоль DeviceLock Management Console имеет встроенный просмотрщик событий, который предлагает более удобную форму представления информации из стандартного журнала Windows. За дополнительной информацией обратитесь к разделу Просмотрщик журнала аудита (для компьютера).

Для просмотра данных аудита, хранимых на сервере DeviceLock Enterprise Server, используйте Просмотрщик журнала аудита (для сервера).

Кроме того, существует расширение стандартной функции аудита, называемое теневым копированием - возможность сохранять точную копию данных, копируемых пользователем, на внешние устройства хранения данных и передаваемых через COM и LPT-порты. Сохраняются точные копии всех файлов и данных. Данные теневого копирования сохраняются в локальной папке, заданной параметром Локальная директория. Данные теневого копирования могут быть переданы на DeviceLock Enterprise Server, заданный параметром DeviceLock Enterprise Server(ы), для хранения в SQL-базе данных.

Для просмотра локально сохраненных данных теневого копирования используйте просмотрщик, встроенный в консоль DeviceLock Management Console. За дополнительной информацией обращайтесь к разделу Просмотрщик журнала теневого копирования (для компьютера).

Для просмотра данных теневого копирования, хранимых на DeviceLock Enterprise Server'е, используйте Просмотрщик журнала теневого копирования (для сервера).

Установка правил аудита и теневого копирования

Чтобы установить правила аудита и теневого копирования для типа устройства, выделите его (для одновременного выделения нескольких типов устройств используйте клавиши Ctrl и/или Shift) и выберите команду **Установить аудит, теневое копирование и алерты** или **Установить офлайновый аудит, теневое копирование и алерты** из контекстного меню, либо нажмите соответствующую кнопку на панели инструментов.

Примечание: Можно задавать различные правила аудита и теневого копирования для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Правила аудита и теневого копирования для оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Правила аудита и теневого копирования для автономного режима (офлайн-профиль) применяются, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Описание политик DeviceLock для автономного режима можно найти в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по настройке правил аудита и теневого копирования см. в разделе Управление правилами аудита, теневого копирования и оповещений для автономного режима.

Если в DeviceLock Group Policy Manager или DeviceLock Service Settings Editor нужно сбросить правила аудита и теневого копирования для оперативного режима в состояние "не задано", выберите команду **Сбросить** из контекстного меню.

Чтобы сбросить правила аудита и теневого копирования, заданные для автономного режима, в состояние "не задано", выберите команду **Сбросить офлайновые настройки** из контекстного меню. Если правила для автономного режима не заданы, к клиентским компьютерам, находящимся не в сети, применяются правила, заданные для оперативного режима.

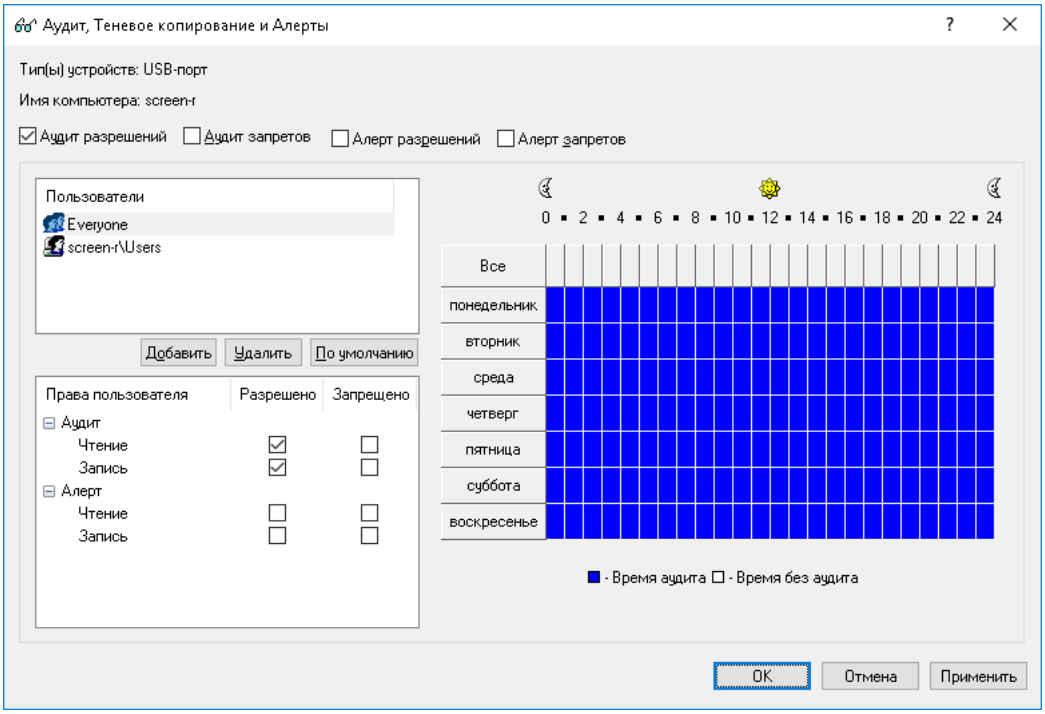
Если в DeviceLock Group Policy Manager или DeviceLock Service Settings Editor требуется заблокировать наследование правил аудита и теневого копирования, заданных для автономного режима, чтобы принудительно применить правила, заданные для оперативного режима, выберите команду **Удалить офлайновые настройки** из контекстного меню.

Аудит, правила теневого копирования и алерты для оперативного режима могут иметь одно из следующих состояний:

- **Не определено** - Аудит, правила теневого копирования и тревожные оповещения для данного типа устройств не заданы.
- **Задано** - Для данного типа устройств заданы аудит, правила теневого копирования и/или тревожные оповещения.
- **Нет аудита** - Настройки для данного типа устройств не разрешают аудит, теневое копирование и тревожные оповещения ни для каких учетных записей.

Диалоговое окно “Аудит, Теневое копирование и Алерты”

Чтобы установить правила аудита и теневого копирования для оперативного режима для определенного типа устройств, выделите тип устройства (для одновременного выделения нескольких типов используйте клавиши Ctrl и/или Shift) и, щелкнув правой кнопкой мыши, выберите пункт **Установить аудит, теневое копирование и алерты** из контекстного меню, либо нажмите соответствующую кнопку на панели инструментов.



Для каждого устройства можно протоколировать два типа попыток доступа:

- **Разрешено** - Все попытки доступа, которые были разрешены сервисом DeviceLock, т.е. пользователю был предоставлен доступ к устройству.
- **Запрещено** - Все попытки доступа, которые были заблокированы сервисом DeviceLock, т.е. пользователю был запрещен доступ к устройству.

Для того чтобы включить протоколирование одного или обоих типов доступа, установите флажки **Аудит разрешений** и/или **Аудит запретов**. Эти флажки не имеют логической привязки к отдельным учетным записям пользователей или групп, они влияют на весь тип устройства.

Имена пользователей и групп пользователей, назначенных данному типу устройства, отображаются в списке учетных записей в левой верхней части диалога **Аудит, Теневое копирование и Алерты**.

Чтобы добавить нового пользователя или группу пользователей в список учетных записей, нажмите кнопку **Добавить**. Вы можете добавить несколько учетных записей одновременно.

Для удаления учетных записей из списка используйте кнопку **Удалить**. Для одновременного удаления нескольких записей используйте клавиши Ctrl и/или Shift.

С помощью кнопки **По умолчанию** можно задать правила аудита и теневого копирования по умолчанию для устройств: члены группы **Пользователи** (Users) и учетная запись **Все** (Everyone) имеют права **Чтение** и **Запись** на аудит, а права на теневое копирование для них отключены.

Используя специальный элемент управления для выбора времени, можно задать период, когда правило аудита для выбранного пользователя или группы будет (или не будет) активно. Этот элемент управления расположен в правой части диалогового окна. Нажимайте левую кнопку мыши для выбора времени, когда правило аудита активно. Для выбора времени, когда правило аудита неактивно, нажимайте правую кнопку. Можно также использовать клавиатуру: стрелки для навигации и пробел для переключения между активным/неактивным состоянием.

Чтобы указать действия пользователя, подлежащие регистрации, задайте соответствующие права. Предусмотрены две группы прав:

- **Аудит** - Права для протоколирования действий пользователя в журнал аудита. Подробнее см. в разделе Группа прав "Аудит".
- **Теневое копирование** - Права для протоколирования действий пользователя в журнал теневого копирования. Подробнее см. в разделе Группа прав "Теневое копирование".

> **Примечание:** Если передача данных запрещена на уровне типа (с помощью разрешений), то теневая копия передаваемых данных не будет создана, так как в этом случае DeviceLock блокирует передачу данных до начала их перехвата. Исключение: Если данные проверяются контентно-зависимыми правилами, то DeviceLock создает теневую копию данных, даже если их передача запрещена на уровне типа.

Рекомендации

Записи в журнале аудита могут не создаваться, несмотря на заданные правила аудита. Данная проблема обычно вызвана тем, что в настройках правил аудита не установлены флажки **Аудит разрешений** и **Аудит запретов**. Существующая конфигурация протоколирования в этом случае не является корректной, что приводит к отсутствию записей в журнале аудита.

При настройке правил аудита необходимо убедиться, что установлен хотя бы один из флажков **Аудит разрешений** и **Аудит запретов**.

Следует также иметь в виду, что протоколирование событий аудита на уровне интерфейса USB не ведётся для устройств, добавленных в белый список (см. Белый список USB-устройств (обычный профиль)), а также для устройств, контроль которых отключен настройками безопасности (см. Настройки безопасности (обычный профиль)).

Группа прав “Аудит”

Права из группы **Аудит** позволяют указать, какие действия требуется регистрировать в журнале аудита. Предусмотрены следующие права аудита:

- **Чтение** - Протоколируются попытки пользователя читать данные. Для типов BlackBerry-устройства, Bluetooth, FireWire-порт, ИК-порт, Параллельный порт, Последовательный порт, USB-порт и WiFi это право можно установить, только если установлено право **Запись** из группы **Аудит**.
- **Запись** - Протоколируются попытки пользователя записывать данные. Для типов BlackBerry-устройства, Bluetooth, FireWire-порт, ИК-порт, Параллельный порт, Последовательный порт, USB-порт и WiFi это право можно установить, только если установлено право **Чтение** из группы **Аудит**.
- **Форматирование** - Протоколируются попытки прямого обращения с записью (т.е. форматирование). Данное право применимо только к следующим типам: Гибкий диск, Жесткий диск, Съемные устройства.
- **Печать** - Протоколируются попытки пользователя посылать документы на принтеры. Данное право применимо только к типу Принтер.
- **Выполнение** - Протоколируются попытки пользователя удаленно выполнить код на стороне устройства. Данное право применимо только к типу Windows Mobile.
- **Чтение не файлов** - Протоколируются попытки пользователя читать не файловые объекты (“Календарь”, “Контакты”, “Задачи” и т. п.). Данное право применимо только к типам iPhone-устройства, Windows Mobile и Palm.
- **Запись не файлов** - Протоколируются попытки пользователя записывать не файловые объекты (“Календарь”, “Контакты”, “Задачи” и т. п.). Данное право применимо только к типам iPhone-устройства, Windows Mobile и Palm.
- **Копирование** - Протоколируются попытки пользователя вставить данные из буфера обмена и сделать снимки экрана. Применимо только к типу Буфер обмена.
- **Чтение с подключенного диска** - Протоколирование всех попыток чтения данных с подключенных дисков в терминальной сессии. Применимо только к типу TC-устройства.
- **Запись на подключенный диск** - Протоколирование всех попыток записи данных на подключенные диски в терминальной сессии. Применимо только к типу TC-устройства.
- **Доступ к последовательному порту** - Протоколирование всех попыток доступа к последовательным портам во время терминальной сессии. Применимо только к типу TC-устройства.
- **Доступ к USB-устройствам** - Протоколирование всех попыток доступа к USB-устройствам во время терминальной сессии. Применимо только к типу TC-устройства.
- **Буфер обмена входящие данные** - Протоколирование всех попыток вставки различных типов данных (текстовых, графических, аудио, файлов и других) из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу TC-устройства.
- **Буфер обмена исходящие данные** - Протоколирование всех попыток вставки различных типов данных (текстовых, графических, аудио, файлов и других) из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу TC-устройства.

Подробнее о правах аудита для каждого типа устройств см. в разделе Сводка прав аудита и теневого копирования по типам устройств.

Группа прав “Теневое копирование”

Права из группы **Теневое копирование** позволяют указать, какие действия требуется регистрировать в журнале теневого копирования. Предусмотрены следующие права теневого копирования:

- **Чтение** - Включается теневое копирование для всех данных, считываемых пользователем. Применимо только к типу MTP.
- **Запись** - Включается теневое копирование для всех данных, записываемых пользователем. Данное право применимо только к следующим типам: Гибкий диск, iPhone-устройства, MTP, Оптический привод, Параллельный порт, Съемные устройства, Последовательный порт, Windows Mobile и Palm.
- **Форматирование** - Включается теневое копирование бинарных данных, записанных пользователем посредством прямого доступа к диску (т.е. форматирование). Данное право применимо только к типам Гибкий диск и Съемные устройства.
- **Печать** - Включается теневое копирование для всех документов, посылаемых на принтеры. Эти документы будут доступны для просмотра (см. описание команды Открыть в разделе Просмотрщик журнала теневого копирования (для компьютера)). Данное право применимо только к типу Принтер.
- **Запись не файлов** - Включается теневое копирование для всех не файловых объектов (календарь, контакты, задачи и т.п.), записываемых пользователем. Данное право применимо только к типам iPhone-устройства, Windows Mobile и Palm.
- **Запись на подключенный диск** - Включается теневое копирование для всех данных, записываемых на подключенные диски в терминальной сессии. Применимо только к типу TC-устройства.
- **Копирование** - Включается теневое копирование данных, вставленных из буфера обмена, а также скриншотов. Применимо только к типу Буфер обмена.
- **Буфер обмена входящие данные** - Включается теневое копирование данных из буфера обмена, вставленных в окно терминальной сессии/виртуальной машины. Применимо только к типу TC-устройства.
- **Буфер обмена исходящие данные** - Включается теневое копирование данных из буфера обмена, вставленных из окна терминальной сессии/виртуальной машины. Применимо только к типу TC-устройства.

Подробнее о правах теневого копирования для каждого типа устройств см. в разделе Сводка прав аудита и теневого копирования по типам устройств.

Сводка прав аудита и теневого копирования по типам устройств

В данном разделе представлен список прав аудита и теневого копирования для каждого типа устройств, а также описана информация, регистрируемая в соответствующих журналах. Для каждого события в журнал записываются следующие сведения: тип события; дата и время, когда событие произошло; тип устройства, на котором произошло событие; причина возникновения события; имя пользователя и процесс, вызвавший событие. Кроме того, регистрируется дополнительная информация о событиях, зависящая от типа устройства:

- BlackBerry-устройства
- Bluetooth
- Буфер обмена
- FireWire-порт
- Гибкий диск
- Жесткий диск
- ИК-порт
- iPhone-устройства
- MTP
- Оптический привод
- Palm
- Параллельный порт
- Принтер
- Съемные устройства
- Последовательный порт
- Ленточные накопители
- TC-устройства
- USB-порт
- WiFi
- Windows Mobile

BlackBerry-устройства

Права, применимые к типу BlackBerry-устройства:

- Аудит: Чтение

  В журнал аудита записывается событие "Доступ к устройству".

- Аудит: Запись

  В журнал аудита записывается событие "Доступ к устройству".

Bluetooth

Права, применимые к типу Bluetooth:

- Аудит: Чтение

  В журнал аудита записывается событие "Доступ к устройству".

- Аудит: Запись

  В журнал аудита записывается событие "Доступ к устройству".

Буфер обмена

Права, применимые к типу Буфер обмена:

- Аудит: Копирование

  В журнал аудита записываются события "Копирование текста", "Копирование файла", "Копирование изображения", "Копирование аудио данных", "Копирование RTF (Изображение)", "Копирование RTF (Файл)", "Копирование RTF (Текст, Изображение)", "Копирование RTF (Текст, Файл)", "Копирование RTF (Изображение, Файл)", "Копирование RTF (Текст, Изображение, Файл)", "Копирование неидентифицированного содержимого", "Копирование экрана", имена файлов, имя процесса и PID.

- Теневое копирование: Копирование

  В журнал теневого копирования записываются все данные, посылаемые в буфер обмена.

FireWire-порт

Права, применимые к типу FireWire-порт:

- Аудит: Чтение

  В журнал аудита записываются события "Подключение", "Отключение" и "Доступ к устройству", имена и ID устройств.

- Аудит: Запись

  В журнал аудита записываются события "Подключение", "Отключение" и "Доступ к устройству", имена и ID устройств.

Гибкий диск

Права, применимые к типу Гибкий диск:

- Аудит: Чтение

  В журнал аудита записываются события "Чтение", "Монтирование", "Размонтирование" и имена файлов.

- Аудит: Запись

  В журнал аудита записываются события "Удаление", "Запись", "Восстановление", "Переименование" и имена файлов.

- Аудит: Форматирование

  В журнал аудита записывается событие "Форматирование" и имя диска.

- Теневое копирование: Запись

  Файлы записываются в журнал теневого копирования.

- Теневое копирование: Форматирование

  Данные без изменений ("как есть") записываются в журнал теневого копирования.

Жесткий диск

Права, применимые к типу Жесткий диск:

- Аудит: Чтение

  В журнал аудита записывается событие "Чтение" и имена файлов.

- Аудит: Запись

  В журнал аудита записываются события "Запись", "Переименование", "Удаление" и имена файлов.

- Аудит: Форматирование

  В журнал аудита записывается событие "Форматирование" и имя диска.

ИК-порт

Права, применимые к типу ИК-порт:

- Аудит: Чтение

  В журнал аудита записывается событие "Доступ к устройству".

- Аудит: Write

  В журнал аудита записывается событие "Доступ к устройству".

iPhone-устройства

Права, применимые к типу iPhone-устройства:

- Аудит: Чтение

  В журнал аудита записывается событие "Чтение файла" и имена файлов.

- Аудит: Запись

  В журнал аудита записываются события "Запись файла", "Переименование файла", "Удаление файла" и имена файлов.

- Аудит: Чтение не файлов

  В журнал аудита записываются события "Чтение бэкапа", "Чтение календаря", "Чтение контакта", "Чтение избранного", "Чтение медиа-данных", "Чтение электронной почты", "Чтение заметки" и имена объектов.

- Аудит: Запись не файлов

  В журнал аудита записываются события "Запись календаря", "Удаление календаря", "Запись контакта", "Удаление контакта", "Запись избранного", "Удаление избранного", "Запись электронной почты", "Удаление электронной почты", "Запись бэкапа", "Запись заметки", "Удаление заметки", "Запись медиа-данных", "Переименование медиа-данных", "Удаление медиа-данных" и имена объектов.

- Теневое копирование: Запись

  Файлы записываются в журнал теневого копирования.

- Теневое копирование: Запись не файлов

  Все не-файловые объекты (календарь, контакты и т.п.) записываются в журнал теневого копирования.

MTP

Права, применимые к типу MTP:

- Аудит: Чтение

  В журнал аудита записывается событие "Чтение" и имена файлов.

- Аудит: Запись

  В журнал аудита записываются события "Удаление", "Переименование", "Запись" и имена файлов.

- Теневое копирование: Чтение

  Файлы записываются в журнал теневого копирования.

- Теневое копирование: Запись

  Файлы записываются в журнал теневого копирования.

Оптический привод

Права, применимые к типу Оптический привод:

- Аудит: Чтение

  В журнал аудита записываются события "Чтение" и "Извлечение" и имена файлов.

- Аудит: Запись

  В журнал аудита записываются события "Запись" и "Форматирование" и имена файлов.

- Теневое копирование: Запись

  В журнал теневого копирования записываются CD/DVD/BD -образы в формате CUE и/или файлы.

Palm

Права, применимые к типу Palm:

- Аудит: Чтение

  В журнал аудита записывается событие "Чтение файла", имена файлов и флаг Sync.

- Аудит: Запись

  В журнал аудита записывается событие "Запись файла", имена файлов и флаг Sync.

- Аудит: Чтение не файлов

  В журнал аудита записываются события "Чтение календаря", "Чтение контакта", "Чтение расхода", "Чтение электронной почты", "Чтение документа", "Чтение памятки", "Чтение блокнота", "Чтение задачи", "Чтение медиа-данных" и имена объектов.

- Аудит: Запись не файлов

  В журнал аудита записываются события "Запись календаря", "Запись контакта", "Запись расхода", "Запись документа", "Запись электронной почты", "Запись памятки", "Запись блокнота", "Запись задачи", "Запись медиа-данных", "Установка" и имена объектов.

- Теневое копирование: Запись

  Файлы записываются в журнал теневого копирования.

- Теневое копирование: Запись не файлов

  Все не-файловые объекты (календарь, контакты, задачи и т.п.) записываются в журнал теневого копирования.

Параллельный порт

Права, применимые к типу Параллельный порт:

- Аудит: Чтение

  В журнал аудита записывается событие "Доступ к устройству".

- Аудит: Запись

  В журнал аудита записывается событие "Доступ к устройству".

- Теневое копирование: Запись

  Все данные, посылаемые в порт, записываются в журнал теневого копирования.

Принтер

Права, применимые к типу Принтер:

- Аудит: Печать

  В журнал аудита записывается событие "Печать", а также имена документов и принтера.

- Теневое копирование: Печать

  Все данные, посылаемые на принтер, записываются в журнал теневого копирования в формате PDF.

Съемные устройства

Права, применимые к типу Съемные устройства:

- Аудит: Чтение

  В журнал аудита записываются события "Чтение", "Чтение зашифрованного", "Извлечение", "Монтирование", "Размонтирование" и имена файлов.

- Аудит: Запись

  В журнал аудита записываются события "Удаление", "Удаление зашифрованного", "Переименование", "Переименование зашифрованного", "Запись", "Запись зашифрованного", "Восстановление", "Восстановление зашифрованного" и имена файлов.

- Аудит: Форматирование

  В журнал аудита записываются события "Форматирование", "Форматирование зашифрованного" и имя диска.

- Теневое копирование: Запись

  Файлы записываются в журнал теневого копирования.

- Теневое копирование: Форматирование

  Данные без изменений ("как есть") записываются в журнал теневого копирования.

Последовательный порт

Права, применимые к типу Последовательный порт:

- Аудит: Чтение

  В журнал аудита записывается событие "Доступ к устройству".

- Аудит: Запись

  В журнал аудита записывается событие "Доступ к устройству".

- Теневое копирование: Запись

  Все данные, посылаемые в порт, записываются в журнал теневого копирования.

Ленточные накопители

Права, применимые к типу Ленточные накопители:

- Аудит: Чтение

  В журнал аудита записываются события "Чтение", "Извлечение" и имена устройств.

- Аудит: Запись

  В журнал аудита записывается событие "Запись" и имена устройств.

ТС-устройства

Права, применимые к типу ТС-устройства:

- Аудит: Чтение с подключенного диска

  В журнал аудита записывается событие "Чтение", имя диска и путь к файлу.

- Аудит: Запись на подключенный диск

  В журнал аудита записывается событие "Запись", имя диска и путь к файлу.

- Аудит: Доступ к последовательному порту

  В журнал аудита записывается событие "Доступ к устройству" и имя последовательного порта.

- Аудит: Доступ к USB-устройствам

  В журнал аудита записывается событие "Доступ к устройству" и имя устройства.

- Аудит: Буфер обмена входящие данные

  В журнал аудита записываются события "Входящий текст", "Входящее изображение", "Входящие аудио данные", "Входящий файл", "Входящий RTF (Изображение)", "Входящий RTF (Файл)", "Входящий RTF (Текст, Изображение)", "Входящий RTF (Текст, Файл)", "Входящий RTF (Изображение, Файл)", "Входящий RTF (Текст, Изображение, Файл)", "Входящие неизвестные данные", имя файла или объекта данных, а также имя процесса и PID.

- Аудит: Буфер обмена исходящие данные

  В журнал аудита записываются события "Исходящий текст", "Исходящее изображение", "Исходящие аудио данные", "Исходящий файл", "Исходящий RTF (Изображение)", "Исходящий RTF (Файл)", "Исходящий RTF (Текст, Изображение)", "Исходящий RTF (Текст, Файл)", "Исходящий RTF (Изображение, Файл)", "Исходящий RTF (Текст, Изображение, Файл)", "Исходящие неизвестные данные", имя файла или объекта данных, а также имя процесса и PID.

- Теневое копирование: Запись на подключенный диск

  Файлы записываются в журнал теневого копирования.

- Теневое копирование: Буфер обмена входящие данные

  Все данные, вставленные из буфера обмена, записываются в журнал теневого копирования.

- Теневое копирование: Буфер обмена исходящие данные

  Все данные, посылаемые в буфер обмена, записываются в журнал теневого копирования.

USB-порт

Права, применимые к типу USB-порт:

- Аудит: Чтение

  В журнал аудита записываются события "Подключение", "Отключение", "Доступ к устройству", а также имена и ID устройств.

- Аудит: Запись

  В журнал аудита записываются события "Подключение", "Отключение", "Доступ к устройству", а также имена и ID устройств.

WiFi

Права, применимые к типу WiFi:

- Аудит: Чтение

  В журнал аудита записывается событие “Доступ к устройству”.

- Аудит: Запись

  В журнал аудита записывается событие “Доступ к устройству”.

Windows Mobile

Права, применимые к типу Windows Mobile:

- Аудит: Чтение

  В журнал аудита записывается событие “Чтение файла”, имена файлов и флаг Sync.

- Аудит: Запись

  В журнал аудита записываются события “Запись файла”, “Удаление файла”, “Переименование”, “Перезапись”, “Создание ярлыка”, а также имена файлов и флаги.

- Аудит: Выполнение

  В журнал аудита записываются события “Вызов” и “Выполнение”, а также имена файлов и названия функций (процедур).

- Аудит: Чтение не файлов

  В журнал аудита записываются события “Чтение календаря”, “Чтение контакта”, “Чтение избранного”, “Чтение электронной почты”, “Чтение вложения”, “Чтение заметки”, “Чтение задачи”, “Чтение медиа-данных”, “Чтение БД Pocket Access”, “Чтение неидентифицированного содержимого”, а также и имена объектов.

- Аудит: Запись не файлов

  В журнал аудита записываются события “Запись календаря”, “Удаление календаря”, “Запись контакта”, “Удаление контакта”, “Запись избранного”, “Удаление избранного”, “Запись электронной почты”, “Удаление электронной почты”, “Запись вложения”, “Удаление вложения”, “Запись заметки”, “Удаление заметки”, “Запись задачи”, “Удаление задачи”, “Запись медиа-данных”, “Удаление медиа-данных”, “Запись БД Pocket Access”, “Удаление БД Pocket Access”, “Запись неидентифицированного содержимого”, “Удаление неидентифицированного содержимого”, а также имена объектов.

- Теневое копирование: Запись

  Файлы записываются в журнал теневого копирования.

- Теневое копирование: Запись не файлов

  Все не файловые объекты (календарь, контакты, задачи и т.п.) записываются в журнал теневого копирования.

Включение алертов

Диалоговое окно “Аудит, Теневое копирование и Алерты” также позволяет включить алерты (тревожные оповещения), которые будут рассылаться при попытке пользователя обратиться к устройству определенного типа.

DeviceLock рассылает тревожные оповещения с учетом настроек оповещений. В этих настройках задается адресат и причина отправки оповещения. Перед тем, как включить оповещения для определенных событий, задайте параметры оповещений в настройках сервиса DeviceLock (см. раздел Алерты).

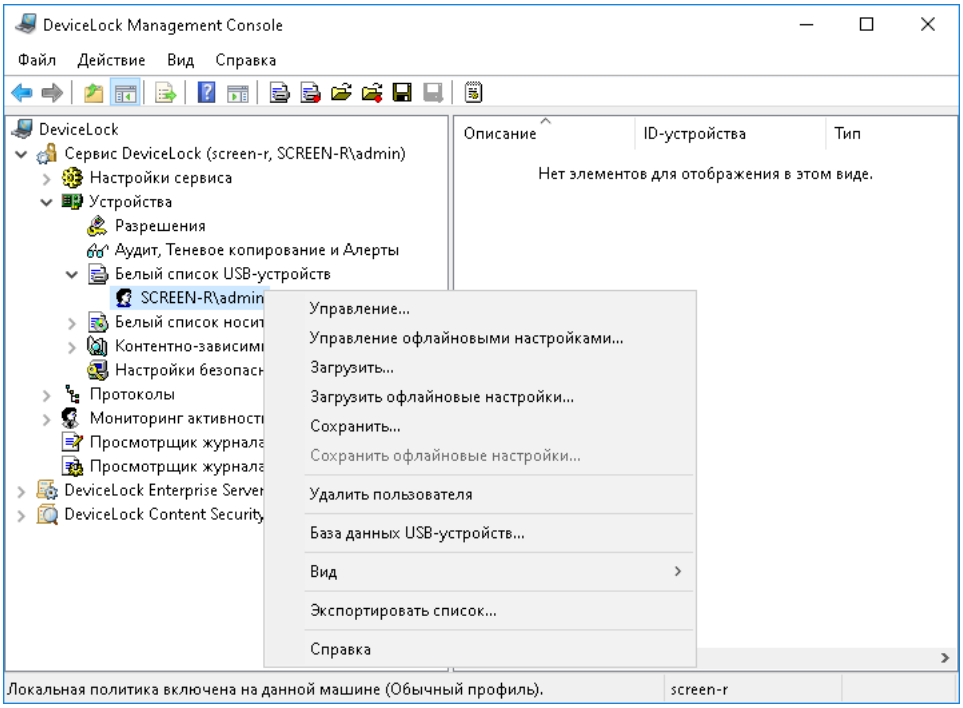
Оповещения о событиях, связанных с доступом, можно включить в диалоговом окне **Аудит, Теневое копирование и Алерты**. Оповещения включаются так же, как задаются правила аудита, в следующем порядке:

- Укажите, для каких событий необходимо рассылать оповещения. Оповещения можно настроить для попыток доступа к устройству (как успешных, так и неуспешных). Установите флажок **Алерт разрешений**, чтобы включить оповещения об успешных попытках доступа к устройству. Установите флажок **Алерт запретов**, чтобы включить оповещения о неудачных попытках доступа к устройству.
- Укажите пользователей и/или группы, на действия которых будут рассылаться оповещения. Для этого в левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.
- Укажите, на какие действия пользователей нужно рассылать оповещения, а на какие нет. В левой верхней части диалогового окна в области **Пользователи** выберите добавленного пользователя или группу. На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить право на оповещение. Права на оповещения определяют, на какие действия пользователя с устройствами следует рассылать оповещения. Права на оповещение аналогичны правам на аудит. Единственное различие состоит в том, что когда происходят события, удовлетворяющие определенным критериям, DeviceLock отправляет тревожное оповещение, а не протоколирует их в журнале аудита. Список прав на аудит для устройств см. в разделе Группа прав “Аудит” ранее в этом документе.
- Укажите дни и часы (например, с 7 утра до 5 вечера с понедельника по пятницу), в которые оповещения о действиях пользователя с устройствами будут или не будут рассылаться. Для этого на правой панели диалогового окна выберите дни и часы левой кнопкой мыши. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда на действия пользователей не будут рассылаться оповещения.

Примечание: Можно настроить различные параметры алертов для оперативного и автономного режимов. Оперативные алерты (обычный профиль) создаются, когда клиентские компьютеры подключены к сети. Автономные алерты (офлайн-профиль) создаются, когда клиентские компьютеры работают в автономном режиме. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Описание политик DeviceLock для автономного режима можно найти в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по настройке алертов см. в разделе Управление правилами аудита, теневого копирования и оповещений для автономного режима.

Белый список USB-устройств (обычный профиль)

Белый список устройств позволяет разрешать использовать только конкретные устройства, которые не будут заблокированы вне зависимости от остальных установок. Это сделано для того, чтобы разрешить использование отдельных устройств при блокировании всех остальных.



В дереве консоли отображается список пользователей и групп, для которых задан белый список устройств. Устройства в белом списке могут быть заданы индивидуально для каждого пользователя и группы. Дополнительную информацию о работе белого списка устройств в DeviceLock можно найти в разделе Управляемый контроль доступа данного руководства.

Контекстное меню белого списка устройств содержит следующие команды:

- **Удалить пользователя** - Удаляет пользователя или группу из белого списка вместе с устройствами, назначенными этому пользователю/группе.
- **Управление** - Открывает диалоговое окно, позволяющее задать или отредактировать белый список для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее задать или отредактировать белый список для автономного режима.
- **Загрузить** - Позволяет импортировать ранее сохраненный файл с белым списком USB-устройств для оперативного режима.
- **Загрузить офлайновые настройки** - Позволяет импортировать ранее сохраненный файл с белым списком USB-устройств для автономного режима.
- **Сохранить** - Позволяет экспортировать белый список USB-устройств, заданный для оперативного режима, в файл с расширением .whl, который затем можно импортировать и использовать на другом компьютере.
- **Сохранить офлайновые настройки** - Позволяет экспортировать белый список USB-устройств, заданный для автономного режима, в файл с расширением .whl, который затем можно импортировать и использовать на другом компьютере.
- **Сбросить** - Сбрасывает белый список USB-устройств для оперативного режима в состояние “не задано”. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

- **Сбросить офлайновые настройки** - Сбрасывает список USB-устройств для автономного режима в состояние “не задано”. Если такой белый список не задан, к клиентским компьютерам, находящимся не в сети, применяется белый список, заданный для оперативного режима.
- **Удалить офлайновые настройки** - Блокирует наследование белого списка, заданного для автономного режима, и принудительно применяет белый список, заданный для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.
- **База данных USB-устройств** - Открывает диалоговое окно, позволяющее добавлять устройства в базу данных USB-устройств для того, чтобы сделать возможным их добавление в белый список.

Примечание: Можно задавать белый список USB устройств для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Белый список USB устройств для оперативного режима (обычный профиль) применяется, когда клиентские компьютеры находятся в сети. Белый список USB устройств для автономного режима (офлайн-профиль) применяется, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Описание политик DeviceLock для автономного режима можно найти в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по настройке белого списка USB-устройств см. в разделе Управление белым списком USB-устройств для автономного режима.

Имеется два варианта идентификации устройств в белом списке:

- **Модель устройства** - Описывает все устройства одной и той же модели. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID) и продукта (PID).

  Комбинация VID и PID описывает конкретную модель, но не конкретное устройство. Это значит, что все устройства данной модели данного производителя будут распознаны как одно устройство.

- **Уникальное устройство** - Описывает конкретное уникальное устройство. Каждое устройство идентифицируется по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера.

  Не каждое устройство имеет собственный серийный номер. Устройство может быть добавлено в белый список как уникальное устройство только в том случае, если производитель присвоил ему серийный номер на этапе изготовления.

Авторизация устройств в белом списке проходит в два этапа:

1. Добавьте устройство в базу данных устройств (см. раздел База данных USB-устройств), чтобы сделать возможным его добавление в белый список.
2. Добавление в белый список. В результате устройство становится авторизованным и для него отключается контроль доступа на уровне интерфейса (USB).

Примечание: Аудит попыток доступа пользователей к устройству, находящемуся в белом списке устройств, не выполняется. Выполняется только аудит попыток пользователей подключить или извлечь устройство, находящееся в белом списке.

Устройства, входящие в белый список

Если выбрать пользователя или группу под узлом **Белый список USB-устройств** в дереве консоли, на панели сведений отображаются устройства, включенные в белый список для этого пользователя или группы.

Контекстное меню устройства в списке на панели сведений содержит следующие команды:

- **Управление** - В зависимости от режима белого списка для данного устройства (оперативный или автономный), открывает диалоговое окно, в котором можно задать белый список устройств для оперативного или автономного режима.
- **База данных USB-устройств** - Открывает диалоговое окно, позволяющее добавлять устройства в базу данных USB-устройств для того, чтобы сделать возможным их добавление в белый список.
- **Переинициализировать** - Установите этот флажок, чтобы обеспечить повторную инициализацию (переподключение) устройства при входе нового пользователя в систему. Некоторые USB-устройства (например, мышь) не могут работать без повторной инициализации, поэтому рекомендуется установить этот флажок для устройств без файловой системы. Также рекомендуется снять этот флажок для устройств хранения данных (флеш-накопители, оптические приводы, внешние жесткие диски и т.п.).

  Внимание: Сервис DeviceLock не может переинициализировать USB-устройства, драйверы которых не позволяют выполнять программное переподключение. При отсутствии доступа к такому устройству из белого списка необходимо извлечь устройство из USB-порта и затем вставить обратно для перезапуска драйвера.

- **Контролировать как тип** - Когда этот флажок установлен, контроль доступа к устройствам, добавленным в белый список, отключается только на уровне интерфейса (USB). Если устройство из белого списка (например, USB-накопитель) относится к обоим уровням - интерфейс (USB) и тип (Съемные устройства), будут применяться разрешения, аудит, теневое копирование и тревожные оповещения на уровне типа (если они есть). В противном случае, если флажок **Контролировать как тип** снят, то контроль доступа к устройствам на уровне типа также отключен. Например, сняв этот флажок для USB-диска, можно избежать проверки прав доступа на уровне типа “Съемные устройства”.
- **Только чтение** - Когда этот флажок установлен, на устройство хранения из белого списка разрешен доступ только на чтение. Если это устройство не поддерживает доступ только на чтение, то доступ будет полностью заблокирован.
- **Разрешить аудит и теневое копирование на уровне типа** - Установите этот флажок, чтобы включить аудит, теневое копирование и оповещения для устройства из белого списка на уровне типа с учетом настроек, заданных для аудита, теневого копирования и алертов, для всех типов, к которым относится это устройство.
- **Удалить** - Удаляет устройство из белого списка для учетной записи пользователя или группы, выбранной в дереве консоли.

Рекомендации

Попытки использовать съемное устройство, добавленное в белый список USB-устройств, могут завершиться ошибкой “Отказано в доступе”. Эта проблема обычно возникает из-за того, что у пользователя нет разрешения на съемные устройства. Обратите внимание, что проверка разрешений для съемных USB-устройств выполняется как на уровне интерфейса (USB-порт), так и на уровне типа (съемное устройство). Если пользователю не разрешено использовать съемные устройства, добавления такого устройства в белый список будет недостаточно, если в белом списке не отключен контроль разрешений по типу устройства.

Для устранения проблемы необходимо предоставить пользователю разрешение на доступ к съемным устройствам (инструкции по установке разрешений см. в разделе Разрешения (обычный профиль)), либо снять флаг **Контролировать как тип** для данного устройства в белом списке.

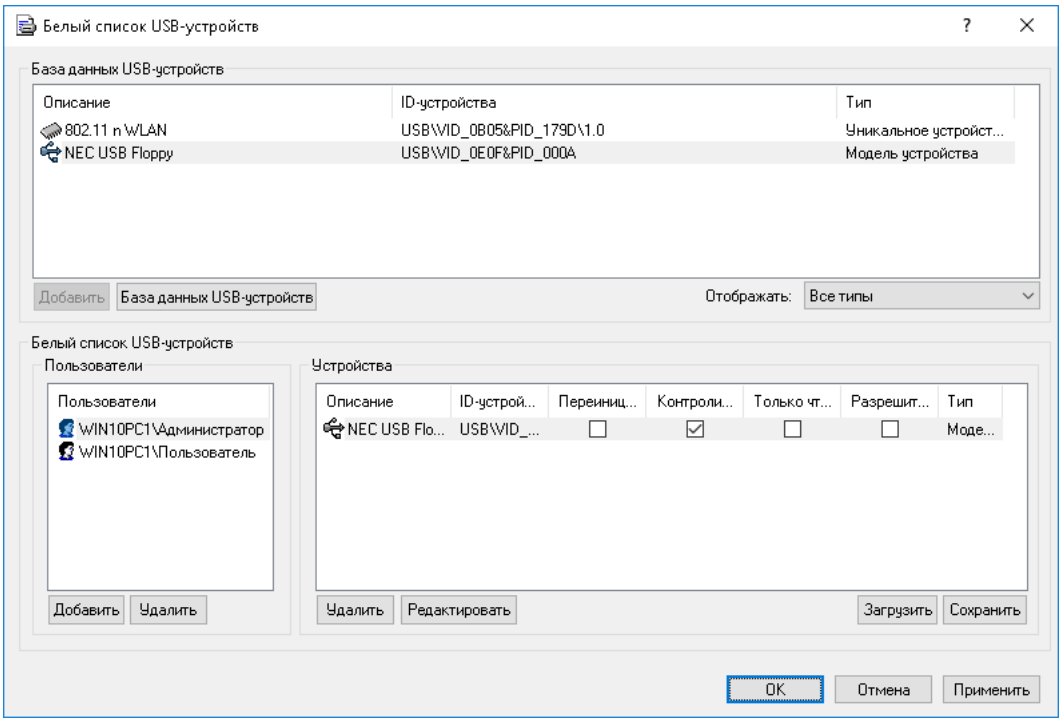
Если одно и то же устройство добавлено в белый список для разных пользователей, то изменение флага **Контролировать как тип** у этого устройства для одного из пользователей изменяет его также для всех пользователей. Флаги **Контролировать как тип** и **Переинициализировать** относятся к устройствам, а не к пользователям, поэтому их изменение действует на всех пользователей, для которых данное устройство добавлено в белый список.

Невозможно по-разному установить флаг **Контролировать как тип** для разных пользователей одного и того же устройства. В качестве обходного пути можно для одних пользователей определить устройство как уникальное, а для других определить его как модель (подробнее об идентификации USB-устройств см. Модель устройства и Уникальное устройство). Так можно создать две записи об устройстве с различными значениями флага **Контролировать как тип**.

Диалоговое окно "Белый список USB-устройств"

Чтобы задать белый список для оперативного режима, выберите пункт **Управление** из контекстного меню либо нажмите соответствующую кнопку на панели инструментов.

В верхней части диалогового окна в списке **База данных USB-устройств** вы можете видеть устройства, добавленные в базу данных.



Как только устройства добавляются из базы данных в белый список определенного пользователя или группы, они становятся разрешенными и ограничение доступа на них не распространяется, когда этот пользователь входит в систему.

Чтобы добавить устройство в список **Белый список USB-устройств**:

1. Выберите соответствующего пользователя (или группу), для которого это устройство должно быть разрешено. Нажмите кнопку **Добавить** под списком **Пользователи**, чтобы добавить учетную запись. Чтобы удалить учетную запись из списка **Пользователи**, нажмите кнопку **Удалить**.

2. Выберите соответствующее устройство в списке **База данных USB-устройств** и нажмите кнопку **Добавить**.

   Если устройство имеет серийный номер, оно может быть добавлено в белый список дважды: как модель устройства и как уникальное устройство. В этом случае модель устройства имеет приоритет над уникальным устройством.

Если флажок **Контролировать как тип** установлен, контроль доступа к устройствам, добавленным в белый список, отключается только на уровне интерфейса (USB). Если устройство из белого списка (например, USB-накопитель) относится к обоим уровням - интерфейс (USB) и тип (съемное устройство), будут применяться разрешения, аудит, теневое копирование и тревожные оповещения (алерты), заданные на уровне типа.

Если флажок **Контролировать как тип** снят, то контроль доступа к устройствам на уровне типа также отключен. Например, сняв флажок **Контролировать как тип** для USB-диска, можно отключить для этого диска проверку разрешений на доступ, заданных для типа **Съемные устройства**.

Примечание: При добавлении составного USB устройства (воспринимаемого системой в виде родительского и дочерних устройств-компонентов) в белый список нужно учитывать, следующее:

- Если в белый список добавлен любой компонент составного USB устройства, контроль доступа отключается для всех компонентов этого устройства на уровне интерфейса (USB-порта). При этом, если внесенное в белый список устройство относится к обоим уровням - интерфейс (USB) и тип (например, съемное устройство), и установлен флажок **Контролировать как тип**, то разрешения (если они заданы) на уровне типа устройства будут применяться в любом случае.

Если установлен флажок **Только чтение**, то на устройство хранения из белого списка разрешен доступ только на чтение. Если это устройство не поддерживает доступ только на чтение, то доступ будет полностью заблокирован.

Установите флажок **Разрешить аудит и теневое копирование на уровне типа**, чтобы включить аудит, теневое копирование и тревожные оповещения для устройства из белого списка на уровне типа с учетом настроек, заданных для аудита, теневого копирования и алертов, для всех типов, к которым относится данное устройство.

Установите флажок **Переинициализировать**, чтобы обеспечить повторную инициализацию (переподключение) устройства при входе нового пользователя в систему. Некоторые USB-устройства (например, мышь) не могут работать без повторной инициализации, поэтому рекомендуется установить этот флажок для устройств без файловой системы. Рекомендуется снять этот флажок для устройств хранения данных (флеш-накопители, оптические приводы, внешние жесткие диски и т.п.).

Внимание: Сервис DeviceLock не может переинициализировать USB-устройства, драйверы которых не позволяют выполнять программное переподключение. При отсутствии доступа к такому устройству из белого список необходимо извлечь устройство из USB-порта и затем вставить обратно для перезапуска драйвера.

Для редактирования описания устройства выберите соответствующую запись в списке **Белый список USB-устройств** и нажмите кнопку **Редактировать**.

Примечание: По умолчанию консоль проверяет уникальность описания каждого USB-устройства, предлагая при необходимости изменить описание. От этой проверки можно отказаться, добавив следующее значение в реестр компьютера, на котором работает консоль:

- Ключ: `HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager`
- Значение: `DisableWLNameUniquenessCheck=dword:00000001`

Для удаления записей используйте кнопку **Удалить** (для одновременного выбора нескольких записей можно использовать клавиши Ctrl и/или Shift).

Чтобы сохранить белый список в виде файла, нажмите кнопку **Сохранить** и выберите имя файла. Чтобы загрузить ранее сохраненный белый список, нажмите кнопку **Загрузить** и выберите файл со списком устройств.

Для управления базой данных устройств (см. раздел База данных USB-устройств) нажмите кнопку **База данных USB-устройств**, чтобы открыть диалоговое окно настройки.

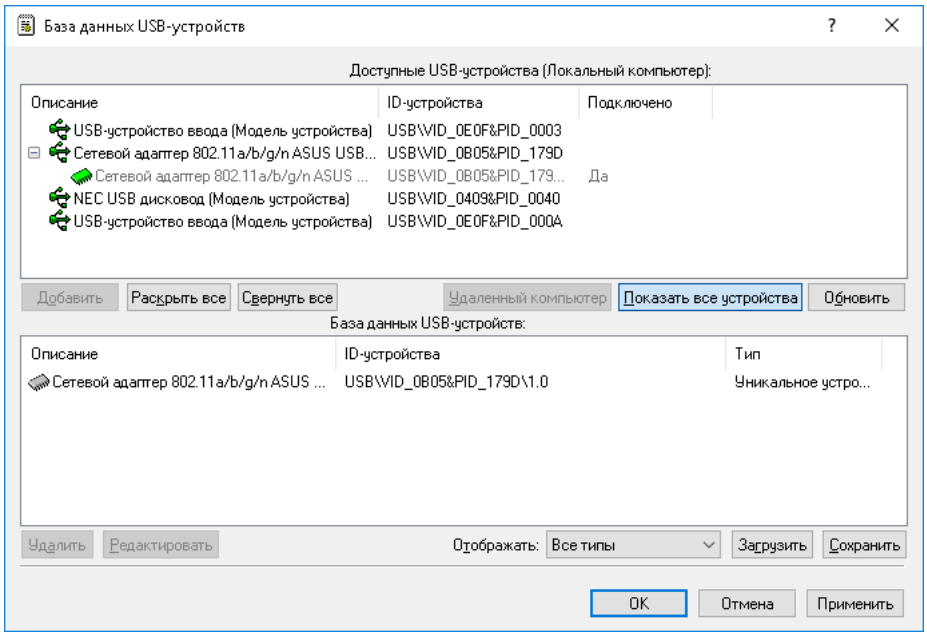
Примечание: При добавлении устройства iPhone в белый список устройств контроль доступа отключается и для iPhone, и для его камеры на уровне интерфейса (USB-порта). Таким образом, невозможно разрешить доступ к iPhone и запретить доступ к его камере на уровне интерфейса (USB-порта). В базе данных устройств устройство iPhone распознается как **Apple Mobile Device USB Driver**.

Однако можно разрешить доступ к камере iPhone, не разрешая доступ к самому устройству. Для этого можно использовать один из следующих способов:

- Способ 1. Чтобы разрешить доступ к камере iPhone, добавьте устройство iPhone в белый список устройств и установите флажок **Контролировать как тип**. Чтобы запретить доступ к устройству iPhone, установите право "любой доступ запрещен" на тип **iPhone-устройства**.
- Способ 2. Чтобы разрешить доступ к камере iPhone, снимите флажок **Управлять доступом к USB-сканерам и устройствам обработки изображения** в настройках безопасности для устройств. Чтобы запретить доступ к устройству iPhone, установите право "любой доступ запрещен" на тип устройств **USB-порт**.

База данных USB-устройств

При помощи диалогового окна **База данных USB-устройств** можно добавлять новые устройства в базу данных и редактировать существующие записи. Перед тем как устройство может быть авторизовано через белый список (см. раздел Белый список USB-устройств (обычный профиль)), оно должно быть добавлено в базу данных.



Вверху диалогового окна находится список **Доступные USB-устройства**. В нем перечислены все устройства, доступные на компьютере. Устройства отображаются в виде простого дерева, в котором родительская запись представляет модель устройства, а потомок - уникальное устройство. Если запись для уникального устройства отсутствует, то это устройство не имеет серийного номера.

Данный список может отображать как подключенные на данный момент устройства (если не нажата кнопка **Показать все устройства**), так и те, которые когда-либо были подключены (если кнопка **Показать все устройства** нажата).

Консоль управления автоматически обновляет список доступных устройств и показывает новые устройства при их подключении. Чтобы обновить этот список вручную, нажмите кнопку **Обновить**.

Чтобы получить список устройств с удаленного компьютера, нажмите кнопку **Удаленный компьютер**. Это кнопка недоступна, когда консоль подключена к локальному компьютеру.

В списке **База данных USB-устройств**, расположенном внизу диалога, перечисляются устройства, уже имеющиеся в базе данных. Добавлять устройства в этот список можно, выбирая записи в списке **Доступные USB-устройства** и нажимая кнопку **Добавить**. Повторное добавление одного и того же устройства невозможно.

Для редактирования описания устройства выберите соответствующую запись в списке **База данных USB-устройств** и нажмите кнопку **Редактировать**.

Примечание: По умолчанию консоль проверяет уникальность описания каждого USB-устройства, предлагая при необходимости изменить описание. От этой проверки можно отказаться, добавив следующее значение в реестр компьютера, на котором работает консоль:

- Ключ: `HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager`
- Значение: `DisableWLNameUniquenessCheck=dword:00000001`

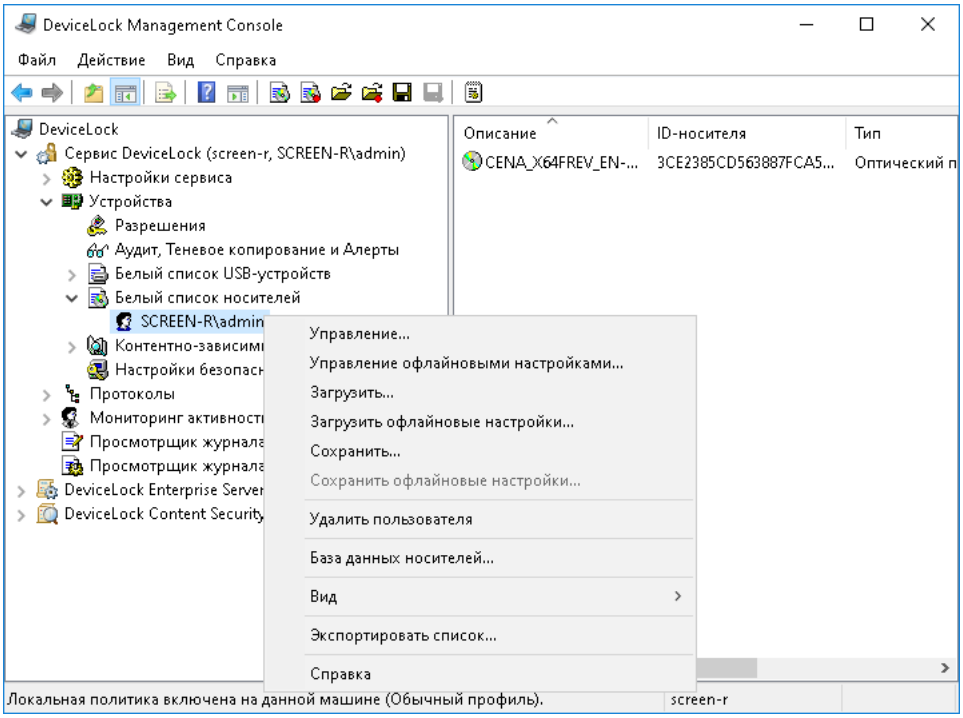
Для удаления записей используйте кнопку **Удалить** (для одновременного выбора нескольких записей можно использовать клавиши Ctrl и/или Shift).

База данных USB-устройств может быть сохранена в виде файла. Для этого нажмите кнопку **Сохранить** и выберите формат файла: .txt либо .csv.

Чтобы загрузить ранее сохраненную базу данных, нажмите кнопку **Загрузить** и выберите файл со списком устройств.

Белый список носителей (обычный профиль)

Белый список носителей позволяет идентифицировать определенный CD/DVD/BD-диск на основе записанных на него данных и разрешить его использование, даже если сам оптический привод заблокирован.



В дереве консоли отображается список пользователей и групп, для которых задан белый список носителей. Носители в белом списке могут быть заданы индивидуально для каждого пользователя и группы.

Контекстное меню белого списка носителей содержит следующие команды:

- **Удалить пользователя** - Удаляет пользователя или группу из белого списка вместе с носителями, назначенными этому пользователю/группе.
- **Управление** - Открывает диалоговое окно, позволяющее задать или отредактировать белый список для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее задать или отредактировать белый список для автономного режима.
- **Загрузить** - Позволяет импортировать ранее сохраненный файл с белым списком носителей для оперативного режима.
- **Загрузить офлайновые настройки** - Позволяет импортировать ранее сохраненный файл с белым списком носителей для автономного режима.
- **Сохранить** - Позволяет экспортировать белый список носителей, заданный для оперативного режима, в файл с расширением .whl, который затем можно импортировать и использовать на другом компьютере.
- **Сохранить офлайновые настройки** - Позволяет экспортировать белый список носителей, заданный для автономного режима, в файл с расширением .whl, который затем можно импортировать и использовать на другом компьютере.
- **Сбросить** - Сбрасывает белый список носителей для оперативного режима в состояние “не задано”. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

- **Сбросить офлайновые настройки** - Сбрасывает список носителей для автономного режима в состояние "не задано. Если такой белый список не задан, к клиентским компьютерам, находящимся не в сети, применяется белый список, заданный для оперативного режима.
- **Удалить офлайновые настройки** - Блокирует наследование белого списка, заданного для актономного режима, и принудительно применяет белый список, заданный для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.
- **База данных носителей** - Открывает диалоговое окно, позволяющее добавлять носители в базу данных для того, чтобы сделать возможным их добавление в белый список.

Примечание: Можно задавать различные белые списки носителей для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Белый список носителей для оперативного режима (обычный профиль) применяется, когда клиентские компьютеры находятся в сети. Белый список носителей для автономного режима (офлайн-профиль) применяется, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Описание политик DeviceLock для автономного режима можно найти в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по настройке белого списка носителей см. в разделе Управление белым списком носителей для автономного режима.

С помощью белого списка можно предоставить доступ к коллекции разрешенных CD/DVD/BD-дисков отдельным пользователям и группам, чтобы только авторизованные пользователи могли работать с разрешенной информацией.

Если авторизованный носитель был скопирован без изменений (побайтовое копирование), то копия также будет авторизованной. Любое изменение в авторизованных данных приведет к изменению уникального идентификатора носителя, и носитель перестанет распознаваться как авторизованный.

Чтобы авторизовать носитель, необходимо:

1. Добавить носитель в базу данных (см. раздел База данных носителей), чтобы сделать возможным его добавление в белый список.
2. Добавить носитель в белый список для определенного пользователя/группы. В результате этот носитель станет авторизованным, и к нему появится доступ на чтение на уровне типа **Оптический привод**.

Примечание: Доступ к носителям, включенным в белый список, может быть открыт только на уровне типа **Оптический привод**. Если же CD/DVD/BD-привод подключается к порту (USB или FireWire) и доступ к этому порту заблокирован, доступ к носителю будет также заблокирован.

Носители, входящие в белый список

Если выбрать пользователя или группу под узлом **Белый список Носителей** в дереве консоли, на панели сведений отображаются носители, включенные в белый список для этого пользователя или группы.

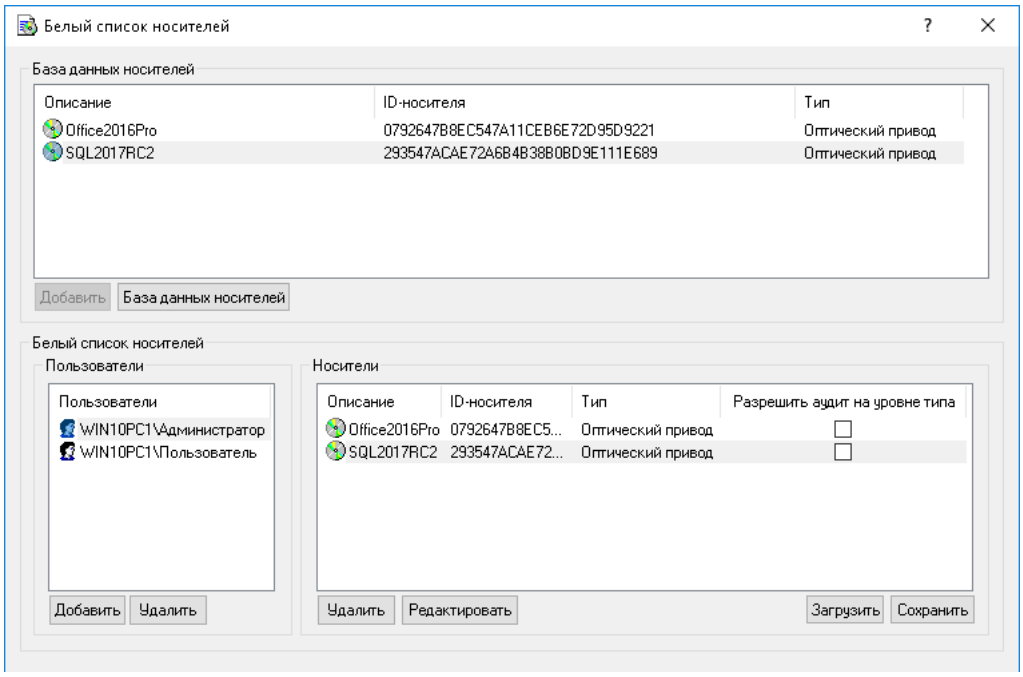
Контекстное меню носителя в списке на панели сведений содержит следующие команды:

- **Управление** - В зависимости от режима белого списка для данного носителя (оперативный или автономный), открывает диалоговое окно, в котором можно задать белый список носителей для оперативного или автономного режима.
- **База данных носителей** - Открывает диалоговое окно, позволяющее добавлять носители в базу данных для того, чтобы сделать возможным их добавление в белый список.
- **Разрешить аудит на уровне типа** - Установите этот флажок, чтобы включить аудит и оповещения для устройства из белого списка на уровне типа с учетом настроек, заданных для аудита, теневого копирования и алертов для типа устройств "Оптический привод".
- **Удалить** - Удаляет носитель из белого списка для учетной записи пользователя или группы, выбранной в дереве консоли.

Диалоговое окно "Белый список носителей"

Чтобы задать белый список носителей для оперативного режима, выберите пункт **Управление** из контекстного меню либо нажмите соответствующую кнопку на панели инструментов.

В верхней части диалогового окна в списке **База данных носителей** вы можете видеть носители, добавленные в базу данных.



Как только носители добавляются из базы данных в белый список определенного пользователя или группы, они становятся разрешенными, и ограничение доступа на них не распространяется, когда этот пользователь входит в систему.

Чтобы добавить носитель в перечень **Белый список носителей**:

1. Выберите соответствующего пользователя (или группу), для которого этот носитель должен быть разрешен. Нажмите кнопку **Добавить** под списком **Пользователи**, чтобы добавить учетную запись. Чтобы удалить учетную запись из списка **Пользователи**, нажмите кнопку **Удалить**.
2. Выберите соответствующий носитель в списке **База данных носителей** и нажмите кнопку **Добавить**.

Установите флажок **Разрешить аудит на уровне типа**, чтобы включить аудит и оповещения для носителей из белого списка с учетом настроек, заданных в Аудит, теневое копирование и алерты (обычный профиль) для типа устройств **Оптический привод**.

Для редактирования описания носителя выберите соответствующую запись в списке **Белый список носителей** и нажмите кнопку **Редактировать**.

Примечание: По умолчанию консоль проверяет уникальность описания каждого носителя, предлагая при необходимости изменить описание. От этой проверки можно отказаться, добавив следующее значение в реестр компьютера, на котором работает консоль:

- Ключ: `HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager`
- Значение: `DisableWLNameUniquenessCheck=dword:00000001`

Для удаления записей используйте кнопку **Удалить** (для одновременного выбора нескольких записей можно использовать клавиши Ctrl и/или Shift).

Чтобы сохранить белый список в виде файла, нажмите кнопку **Сохранить** и выберите имя файла. Чтобы загрузить ранее сохраненный белый список, нажмите кнопку **Загрузить** и выберите файл со списком носителей.

Для управления базой данных носителей (см. раздел База данных носителей) нажмите кнопку **База данных носителей**, чтобы открыть диалоговое окно настройки.

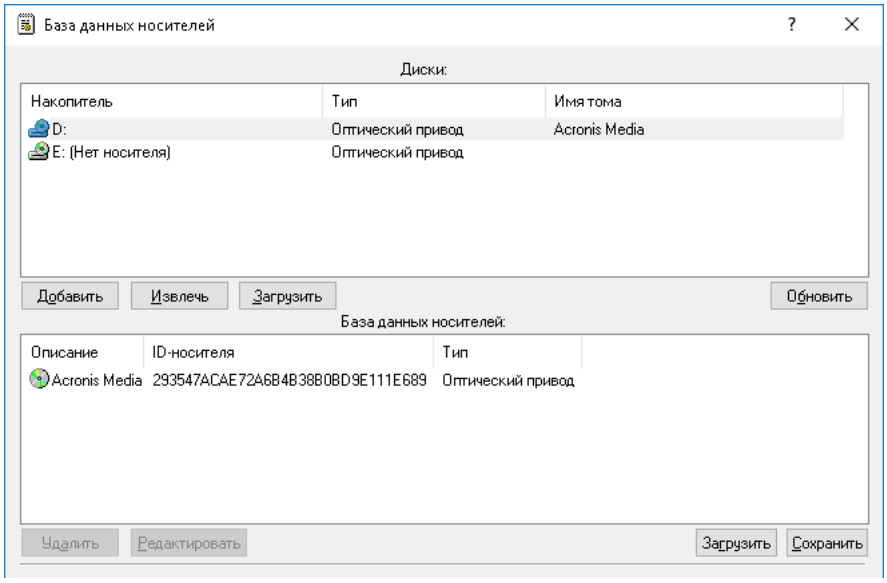
Примечание: С помощью белого списка носителей пользователю можно предоставить доступ только на чтение данных. Невозможно авторизовать носитель для записи.

База данных носителей

В диалоговом окне **База данных носителей** вы можете добавлять новые носители и редактировать записи существующих носителей.

Перед тем как носитель может быть авторизован через белый список (см. раздел Белый список носителей (обычный профиль)), его нужно добавить в базу данных.

В верхней части диалога находится список **Диски**. В нем отображены все устройства локального компьютера, которые могут содержать носители.



Консоль управления автоматически обновляет список доступных носителей и показывает новые носители по мере их появления в устройствах. Чтобы вручную обновить этот список, нажмите кнопку **Обновить**.

В списке, расположенном в нижней части диалога, отображаются носители, которые уже имеются в базе данных.

Вы можете добавлять носители в этот список, выбирая соответствующие записи в списке **Диски** и нажимая кнопку **Добавить**. Авторизация носителя занимает некоторое время, в зависимости от объема данных, записанных на нем. Повторное добавление одного и того же носителя невозможно.

Для редактирования описания носителя выберите соответствующую запись в списке и нажмите кнопку **Редактировать**.

Примечание: По умолчанию консоль проверяет уникальность описания каждого носителя, предлагая при необходимости изменить описание. От этой проверки можно отказаться, добавив следующее значение в реестр компьютера, на котором работает консоль:

- Ключ: `HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager`
- Значение: `DisableWLNameUniquenessCheck=dword:00000001`

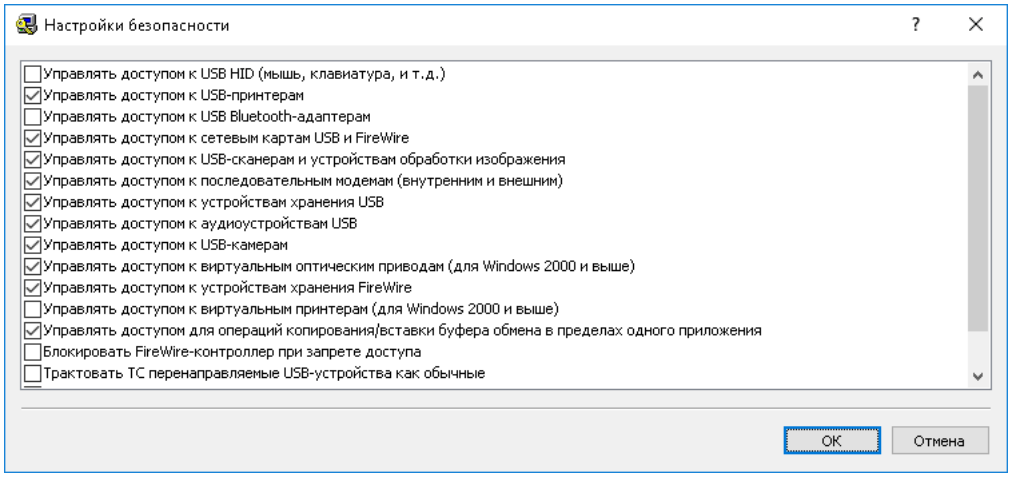
Для удаления записей используйте кнопку **Удалить** (для одновременного выбора нескольких записей можно использовать клавиши Ctrl и/или Shift).

База данных носителей может быть сохранена в виде файла. Для этого нажмите кнопку **Сохранить** и выберите формат файла: .txt либо .csv.

Чтобы загрузить ранее сохраненную базу данных, нажмите кнопку **Загрузить** и выберите файл со списком носителей.

Настройки безопасности (обычный профиль)

DeviceLock предоставляет ряд дополнительных настроек безопасности, которые влияют на разрешения и правила аудита для некоторых типов устройств. Эти настройки позволяют полностью блокировать определенные типы устройств, разрешив при этом использование отдельных классов устройств внутри этих типов. Например, можно полностью закрыть доступ к USB-порту, но разрешить использование любых мышей и клавиатур с USB-интерфейсом. Подробнее см. в разделе Описание настроек безопасности.



Узел “Настройки безопасности”

Этот узел в дереве консоли предназначен для администрирования настроек безопасности для устройств (см. Описание настроек безопасности далее в этом документе).

Контекстное меню узла **Настройки безопасности** содержит следующие команды:

- **Управление** - Открывает диалоговое окно, позволяющее совместно включать или отключать настройки безопасности для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее совместно включать или отключать настройки безопасности для автономного режима.

Примечание: Можно задавать различные настройки безопасности для разных режимов работы (оперативного и автономного). Настройки безопасности для оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Настройки безопасности для автономного режима (офлайн-профиль) применяются, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Описание политик DeviceLock для автономного режима можно найти в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по заданию настроек безопасности см. в разделе Управление настройками безопасности для автономного режима.

Если в дереве консоли выбран узел **Настройки безопасности**, на панели сведений отображается список настроек. Чтобы управлять настройкой, щелкните ее правой кнопкой мыши на панели сведений и используйте команды контекстного меню:

- **Включить** - Включает настройку безопасности для оперативного режима.
- **Выключить** - Отключает настройку безопасности для оперативного режима.
- **Сбросить** - Сбрасывает настройку для оперативного режима в состояние “не задано”. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.
- **Включить офлайн** - Включает настройку безопасности для автономного режима.

- **Выключить офлайн** - Отключает настройку безопасности для автономного режима.
- **Сбросить офлайновые настройки** - Сбрасывает все ранее заданные настройки для автономного режима в состояние "не задано". Если настройки безопасности для автономного режима не заданы, к клиентским компьютерам, находящимся не в сети, применяются настройки безопасности для оперативного режима.
- **Управление** - Открывает диалоговое окно, позволяющее совместно включать или отключать настройки безопасности для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее совместно включать или отключать настройки безопасности для автономного режима.
- **Удалить офлайновые настройки** - Блокирует наследование настроек безопасности для автономного режима и принудительно применяет настройки, заданные для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

Чтобы изменить настройки оперативного режима (обычный профиль), можно дважды щелкнуть соответствующую настройку на панели сведений для изменения ее состояния (**Включено** / **Отключено**). Также можно щелкнуть настройку правой кнопкой мыши и выбрать пункт **Управление** в контекстном меню, или нажать соответствующую кнопку на панели инструментов.

Описание настроек безопасности

DeviceLock предоставляет следующие настройки безопасности для устройств:

- **Управлять доступом к USB HID** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к устройствам ввода (клавиатура, мышь), подключенным к USB-портам. Если настройка отключена, то эти устройства продолжат работу в обычном режиме, и аудит для них также будет отключен.
- **Управлять доступом к USB-принтерам** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к принтерам, подключенным к USB-портам. Если настройка отключена, то даже при заблокированном USB-порте принтеры будут работать в обычном режиме, и аудит для них также будет отключен.
- **Управлять доступом к USB-сканерам и устройствам обработки изображения** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к сканерам и цифровым фотоаппаратам, подключенным к USB-портам. Если настройка отключена, то даже при заблокированном USB-порте эти устройства будут работать в обычном режиме, и аудит для них также будет отключен.
- **Управлять доступом к USB Bluetooth-адаптерам** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к Bluetooth-адаптерам, подключенным к USB-портам. Если настройка отключена, то даже при заблокированном USB-порте Bluetooth-адаптеры будут работать в обычном режиме, и аудит для них также будет отключен.

  Эта настройка влияет только на контроль доступа и аудит на уровне интерфейса (USB). Если устройство принадлежит к обоим уровням, контроль доступа и аудит для уровня типа (Bluetooth) будут выполняться в любом случае.
- **Управлять доступом к устройствам хранения USB** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к устройствам хранения данных (таким как флэш-накопители), подключенным к USB-портам. Если настройка отключена, то даже при заблокированном USB-порте эти устройства будут работать в обычном режиме, и аудит для них также будет отключен.

  Эта настройка влияет только на контроль доступа и аудит на уровне интерфейса (USB). Если устройство принадлежит к обоим уровням, контроль доступа и аудит для уровня типа ("Съемные устройства", "Гибкий диск", "Оптический привод" или "Жесткий диск") будут выполняться в любом случае.

- **Управлять доступом к аудиоустройствам USB** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к аудиоустройствам (например, гарнитурам и микрофонам), подключенным к USB-портам. Если настройка отключена, то даже при заблокированном USB-порте эти устройства будут работать в обычном режиме, и аудит для них также будет отключен.
- **Управлять доступом к USB-камерам** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к веб-камерам, подключенным к USB-портам. Если настройка отключена, то даже при заблокированном USB-порте эти устройства будут работать в обычном режиме, и аудит для них также будет отключен.
- **Управлять доступом к сетевым картам USB и FireWire** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к сетевым картам, подключенным к USB- или FireWire-портам. Если настройка отключена, то даже при заблокированном USB- или FireWire-порте эти устройства будут работать в обычном режиме, и аудит для них также будет отключен.
- **Управлять доступом к устройствам хранения FireWire** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к устройствам хранения данных, подключенным к FireWire-портам. Если настройка отключена, то даже при заблокированном FireWire-порте эти устройства будут работать в обычном режиме, и аудит для них также будет отключен.

  Эта настройка влияет только на контроль доступа и аудит на уровне интерфейса (FireWire). Если устройство принадлежит к обоим уровням, контроль доступа и аудит для уровня типа ("Съемные устройства", "Гибкий диск", "Оптический привод" или "Жесткий диск") будут выполняться в любом случае.
- **Управлять доступом к последовательным модемам (внутренним и внешним)** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к модемам, подключенным к COM-портам. Если настройка отключена, то даже при заблокированном COM-порте эти устройства будут работать в обычном режиме, и аудит для них также будет отключен.
- **Управлять доступом к виртуальным оптическим приводам** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к виртуальным CD/DVD/BD-приводам. Если настройка отключена, то даже при заблокированном DVD/CD/BD-приводе виртуальные диски будут работать в обычном режиме, и аудит для них также будет отключен.
- **Управлять доступом к виртуальным принтерам** - Если включено, то сервис DeviceLock может контролировать и протоколировать отправку документов на виртуальные принтеры, т.е. принтеры, которые печатают не на реальном физическом устройстве, а, например, перенаправляют печать в файл. Если настройка отключена, то даже при заблокированном физическом принтере виртуальные принтеры будут печатать как обычно, и аудит для них также будет отключен.
- **Управлять доступом для операций копирования/вставки буфера обмена в пределах одного приложения** - Если включено, то сервис DeviceLock может контролировать и протоколировать операции копирования/вставки в/из буфера обмена в пределах приложения. Если настройка отключена, то даже при заблокированном буфере обмена операции копирования/вставки в пределах одного приложения будут разрешены, и аудит для них также будет отключен.
- **Блокировать FireWire-контроллер при запрете доступа** - Если включено, то сервис DeviceLock может отключать FireWire-контроллер при запрещении учетной записи **Все** (Everyone) любого доступа к устройствам для типа **FireWire-порт**.
- **Переключать PostScript-принтер в не PostScript-режим** - Если включено, то сервис DeviceLock переводит принтеры PostScript в режим работы обычных принтеров. Это позволяет решить проблему, из-за которой сервис DeviceLock не может корректно выполнить теневое копирование и анализ данных для печати на принтерах, использующих драйвер PostScript.

- **Трактовать ТС перенаправляемые USB-устройства как обычные** - Если включено, то сервис DeviceLock управляет доступом ко всем USB-устройствам, переданным внутрь сеансов Citrix XenDesktop/MS RemoteFX в соответствии с правами, заданными для типа **USB-порт**. В противном случае, сервис DeviceLock будет управлять доступом ко всем USB-устройствам, переданным внутрь сеансов Citrix XenDesktop/MS RemoteFX, в соответствии с набором прав **Доступ к USB-устройствам** для типа **ТС-устройства**.
- **Управлять доступом к Bluetooth HID (мышь, клавиатура, и т.д.)** - Если включено, то сервис DeviceLock может контролировать и протоколировать доступ к устройствам ввода (клавиатура, мышь), подключенным через Bluetooth. Если настройка отключена, то эти устройства продолжат работу в обычном режиме, и аудит для них также будет отключен.

  Эта настройка влияет только на контроль доступа и аудит на уровне типа Bluetooth. Если устройство принадлежит к обоим уровням, контроль доступа и аудит для уровня интерфейса (USB) будут выполняться в любом случае.

Настройки безопасности аналогичны белому списку устройств (см. раздел Белый список USB-устройств (обычный профиль)) за исключением трех моментов:

1. С помощью настроек безопасности можно разрешить доступ только к целому классу устройств. Невозможно открыть доступ только к одному устройству, не разрешая доступ к остальным устройствам этого класса.

   Например, при отключении параметра **Управлять доступом к устройствам хранения USB** становятся доступны все USB-накопители независимо от модели и производителя. Используя настройки безопасности, вы можете разрешить использование целого класса устройств; но вы не можете разрешить использование только одной конкретной модели, пока все остальные устройства этого же класса являются заблокированными.

2. Используя настройки безопасности, вы можете выбрать устройство только из списка предопределенных классов. Если устройство не принадлежит ни одному из предопределенных классов, оно не может быть разрешено через настройки безопасности.

   Например, в настройках безопасности нет отдельного класса для считывателей смарт-карт, поэтому если требуется разрешить доступ к считывателю при заблокированном порте, необходимо воспользоваться белым списком устройств.

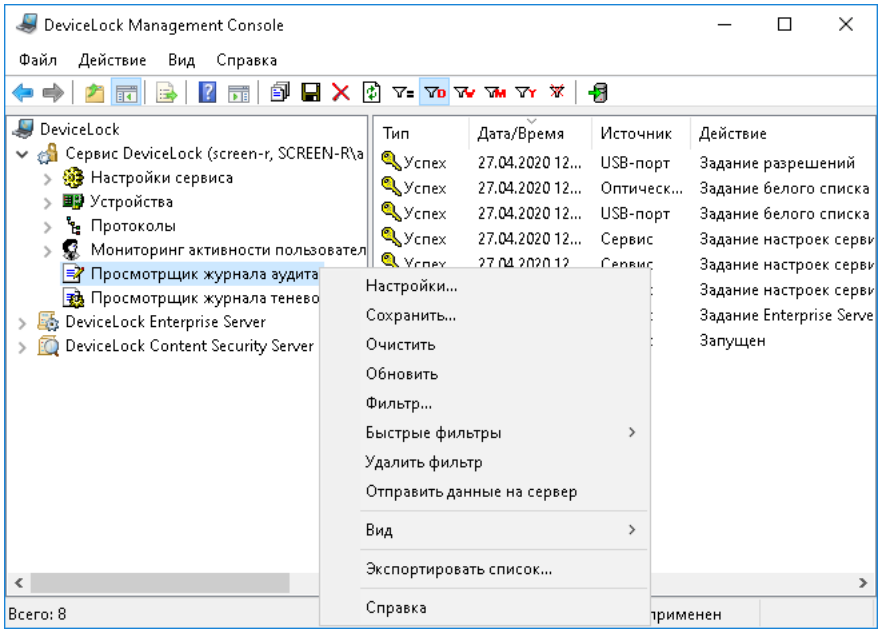
3. Используя настройки безопасности, вы не можете контролировать доступ к устройствам для пользователей или групп. Настройки безопасности влияют сразу на всех пользователей локального компьютера.

Примечание: Настройки безопасности гарантированно работают только для устройств, управляемых стандартными драйверами Windows. Некоторые устройства, использующие драйверы сторонних производителей, не могут быть отнесены сервисом DeviceLock к тому или иному классу. Контроль доступа к таким устройствам невозможно отключить в настройках безопасности. В этом случае можно авторизовать такие устройства по отдельности с помощью белого списка устройств (см. Белый список USB-устройств (обычный профиль)).

Просмотрщик журнала аудита (для компьютера)

Консоль управления содержит встроенный просмотрщик записей аудита, который позволяет просматривать данные аудита из стандартного журнала Windows подключенного компьютера.

Стандартный журнал Windows используется для хранения записей аудита, если у параметра Тип журнала аудита в настройках сервиса установлен флажок **Журнал событий**. Если установлен флажок **Журнал DeviceLock**, то записи аудита хранятся в серверном журнале и могут быть просмотрены с помощью серверного просмотрщика (см. Просмотрщик журнала аудита (для сервера)).



Журнал аудита используется для хранения записей протокола (событий) доступа пользователей к устройствам, подпавшим под заданные правила аудита. Чтобы получить дополнительную информацию, обратитесь к разделу Аудит, теневое копирование и алерты (обычный профиль) данного руководства.

В журнал аудита также записываются все изменения в настройках сервиса DeviceLock, если параметр Записывать события об изменении политики и старте/остановке сервиса установлен в списке Настройки сервиса.

Столбцы просмотрщика определены следующим образом:

- **Тип** - Возможны события следующих типов:
  - **Успех** - DeviceLock позволил выполнить некоторое действие (например, прочитать, записать или передать какой-либо файл или данные).
  - **Отказ** - DeviceLock не позволил выполнить некоторое действие (например, прочитать, записать или передать какой-либо файл или данные).
  - **Информация** - DeviceLock успешно применил некоторое контентно-зависимое правило для обнаружения контента.
  - **Предупреждение** - DeviceLock столкнулся с ситуацией, в которой возможны осложнения или ошибки, если не предпринять никаких действий. Краткое описание проблемы или ситуации, с которой столкнулся DeviceLock, можно найти в поле **Причина** или **Действие**. Например, предупреждение может быть вызвано проблемой, возникшей при применении контентно-зависимого правила для обнаружения контента, в результате чего не удалось проверить содержимое файла, указанного в поле **Имя** записи о событии.
- **Дата/Время** - Дата и время, когда событие было получено сервисом DeviceLock.

- **Источник** - Тип устройства или имя протокола. В качестве источника может также быть указан Сервис, если событие вызвано действием, затрагивающим сервис DeviceLock.
- **Действие** - Действие, вызвавшее событие.
- **Имя** - Имя объекта (файла, USB-устройства и т.п.).
- **Информация** - Прочая относящаяся к данному устройству или протоколу информация о событии, такая как флаги доступа, имя устройства или протокола, ID устройства, описание устройства из базы данных (см. База данных USB-устройств) и т.п.
- **Причина** - Указывает, почему произошло событие или чем оно было вызвано. Возможны следующие значения:
    - **Разрешения устройства** - Событие вызвано попыткой получить доступ, прочитать или записать данные на определенное устройство.
    - **Разрешения протокола** - Событие вызвано попыткой выполнить соединение, отправить или получить данные посредством определенного протокола.
    - **Настройки безопасности** - Событие вызвано срабатыванием некоторой настройки безопасности для устройств или протоколов (см. Описание настроек безопасности для устройств и Описание настроек безопасности для протоколов).
    - **Правило** - Событие вызвано срабатыванием какого-либо контентно-зависимого правила.

      За этим значением обычно следует имя правила и краткое описание совпадений контента, ключевых слов и/или типов файлов, которые привели к срабатыванию этого правила. Например, если правило использует группу ключевых слов, перечисляются слова, на которые оно отреагировало.

      Если правило не удалось выполнить из-за ошибки, предоставляется краткое описание ошибки (например, “Сервер DeviceLock недоступен”, “Сервер DeviceLock слишком занят”, “Поврежденные данные” или “Защищено паролем”).
    - **Белый список** - Событие вызвано устройством из белого списка USB-устройств либо срабатыванием некоторого правила белого списка протоколов. За этим значением следует имя данного устройства или правила.
    - **Базовый IP-файрвол** - Событие вызвано срабатыванием некоторого правила базового IP-файрвола. За этим значением следует имя данного правила.
    - **Ошибка контентно-зависимых правил** - Событие, обычно указывающее на то, что DeviceLock не смог применить контентно-зависимые правила к некоторому файлу или данным. В результате пользователю было отказано в доступе или передаче этого файла или данных.
    - **Локальная квота исчерпана** - Не удалось применить некоторое правило или создать теневую копию некоторого файла или данных, поскольку размер локальной директории хранения данных превысил локальную квоту (подробнее см. в описании параметра Локальная квота (%)). В результате пользователю было отказано в доступе или передаче этого файла или данных.
    - **Ошибка теневого копирования** - Не удалось создать теневую копию некоторого файла или данных из-за ошибки доступа к локальной директории хранения данных. В результате пользователю было отказано в доступе или передаче этого файла или данных.
    - **Инициализация/Деинициализация** - Событие вызвано одним из следующих условий:
        - Извлечено устройство из USB-порта.
        - Выполнено монтирование или размонтирование съемного устройства.
        - Выполнено соединение с удаленным хостом, обслуживающим несколько веб-протоколов, в ситуации, когда разрешения для протоколов позволяют подключиться к данному хосту, в то время как прочие HTTP-соединения блокируются. При этом в качестве источника события указывается HTTP.

- **Пользователь** - Имя пользователя, связанного с данным событием.
- **PID** - Идентификатор процесса, связанного с событием.
- **Процесс** - Полный путь к исполняемому файлу приложения. В некоторых случаях вместо полного пути может быть показано только имя процесса.

Управление журналом аудита (для компьютера)

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узел **Сервис DeviceLock** и щелкните правой кнопкой мыши **Просмотрщик журнала аудита** под этим узлом.

  - или -

- В дереве консоли DeviceLock Management Console выберите **Сервис DeviceLock** > **Просмотрщик журнала аудита** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале (см. Настройки журнала аудита (для компьютера)).
- **Сохранить** - Сохранить журнал в указанный файл.
- **Очистить** - Удалить все записи о событиях, имеющиеся в журнале на данный момент.

  Эта команда добавляет в журнал запись об удалении, указывающую, сколько записей было удалено, а также кто выполнил удаление и с какого компьютера.

- **Обновить** - Обновить список событий с учетом последних изменений.
- **Фильтр** - Отображать только записи о событиях, которые удовлетворяют заданным условиям (см. Фильтр журнала аудита (для компьютера)).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра событий, произошедших за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

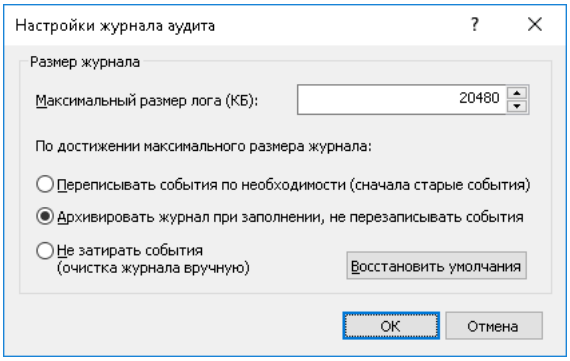
  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).

- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Отправить данные на сервер** - Если в настройках сервиса задан параметр DeviceLock Enterprise Server(ы) и установлен флажок **Журнал DeviceLock** у параметра Тип журнала аудита, то для срочной отправки журнала на сервер можно использовать команду **Отправить данные на сервер**. Поскольку сервер DeviceLock Enterprise Server автоматически собирает данные журналов по мере их накопления сервисом DeviceLock, использовать эту команду не обязательно.

Настройки журнала аудита (для компьютера)

Чтобы определить максимальный размер журнала аудита и действия Windows в случае его заполнения, выберите команду **Настройки** из контекстного меню, доступного по нажатию правой кнопки мыши на элементе **Просмотрщик журнала аудита**, или нажмите кнопку на панели инструментов.



Параметр **Максимальный размер лога** задает максимально допустимый размер журнала (в килобайтах). Файл журнала создается и используется только службой журналов событий Windows. Файл журнала находится в папке `%SystemRoot%\system32\config` и называется `DeviceLo.evt`.

Чтобы определить действия Windows в случае заполнения журнала аудита, выберите одну из этих опций:

- **Переписывать события по необходимости (сначала старые события)** - ОС перезаписывает старые записи новыми, когда превышается размер, заданный в параметре **Максимальный размер лога**.
- **Архивировать журнал при заполнении, не перезаписывать события** - ОС архивирует журнал, когда превышается размер, заданный в параметре **Максимальный размер лога**. Старые записи отправляются в архив, так что они не перезаписываются новыми.
- **Не затирать события (очистка журнала вручную)** - Система не перезаписывает записи, когда превышается размер, заданный в параметре **Максимальный размер лога**, и в таком случае вам необходимо очищать журнал вручную.

Если сервис DeviceLock работает на операционной системе Windows Server 2003, Windows XP или более ранней версии операционной системы Windows, то вместо опции архивирования журнала появляется следующая опция:

- **Затирать события старше чем** <число> **дней** - ОС перезаписывает только те записи, которые старше заданного количества дней.

Примечание: Когда журнал аудита заполнен и в нем нет записей, которые можно было бы удалить, сервис DeviceLock не может писать новые записи в такой журнал.

Чтобы сбросить текущие настройки, нажмите кнопку **Восстановить умолчания**. Настройки по умолчанию выглядят следующим образом:

- Для параметра **Максимальный размер лога** установлено значение 20480 килобайт.

  В случае Windows Server 2003, Windows XP или более ранней версии операционной системы Windows, установлено значение 512 килобайт.

- Выбрана опция **Архивировать журнал при заполнении, не перезаписывать события**.

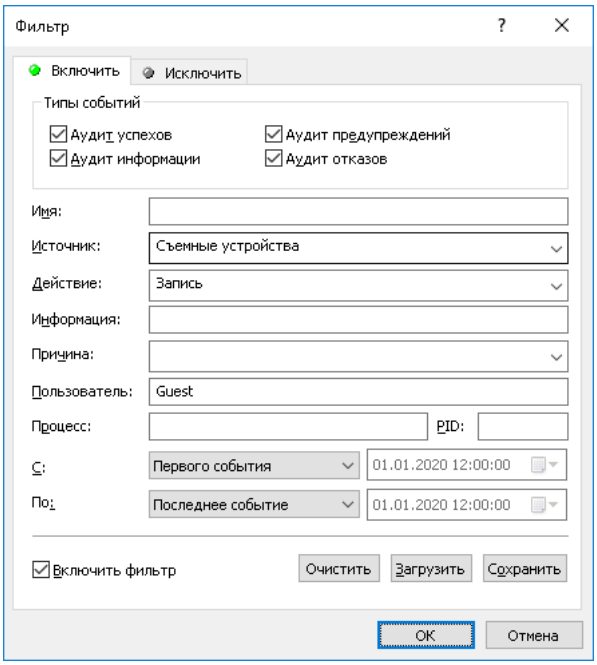
  В случае Windows Server 2003, Windows XP или более ранней версии операционной системы Windows, выбрана опция **Затирать события старше чем** <число> **дней** и для нее установлено значение 7 дней.

Примечание: В консолях DeviceLock Service Settings Editor и DeviceLock Group Policy Manager вместо опции **Архивировать журнал при заполнении, не перезаписывать события** всегда отображается опция **Затирать события старше чем** <число> **дней**, независимо от версии операционной системы, и по умолчанию для параметра **Максимальный размер лога** установлено значение 512 килобайт, выбрана опция **Затирать события старше чем** <число> **дней**, и для нее установлено значение 7 дней.

Фильтр журнала аудита (для компьютера)

Просмотрщик журнала аудита (для компьютера) позволяет отфильтровать данные так, чтобы только записи, удовлетворяющие заданным условиям, выводились в список.

Чтобы открыть диалоговое окно **Фильтр**, выберите команду **Фильтр** из контекстного меню, доступного по нажатию правой кнопки мыши на элементе **Просмотрщик журнала аудита**, или нажмите кнопку ▽ на панели инструментов.



Существует два типа фильтров:

- **Включающие** - В списке отображаются только записи, удовлетворяющие условиям, заданным на вкладке **Включить**.
- **Исключающие** - В списке не отображаются записи, удовлетворяющие условиям, заданным на вкладке **Исключить**.

Чтобы использовать любой тип фильтра, нужно сначала включить его, установив флажок **Включить фильтр**. Чтобы временно выключить фильтр, снимите этот флажок.

Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

Когда фильтр включен, можно настроить условия фильтрации, задав необходимые значения в следующих полях:

- **Типы событий** - Фильтрация по типу событий. Возможны следующие варианты (установите соответствующие флажки):
  - **Аудит успехов** - DeviceLock позволил выполнить некоторое действие (например, прочитать, записать или передать какой-либо файл или данные).
  - **Аудит отказов** - DeviceLock не позволил выполнить некоторое действие (например, прочитать, записать или передать какой-либо файл или данные).
  - **Аудит информации** - DeviceLock успешно применил некоторое контентно-зависимое правило для обнаружения контента.
  - **Аудит предупреждений** - DeviceLock столкнулся с ситуацией, в которой возможны осложнения или ошибки, если не предпринять никаких действий.
- **Имя** - Текст, соответствующий значению столбца **Имя** в просмотрщике журнала аудита. Это поле нечувствительно к регистру.
- **Источник** - Текст, соответствующий значению столбца **Источник** в просмотрщике журнала аудита. Это поле нечувствительно к регистру.
- **Действие** - Текст, соответствующий значению столбца **Действие** в просмотрщике журнала аудита. Это поле нечувствительно к регистру.
- **Информация** - Текст, соответствующий значению столбца **Информация** в просмотрщике журнала аудита. Это поле нечувствительно к регистру.
- **Причина** - Текст, соответствующий значению столбца **Причина** в просмотрщике журнала аудита. Это поле нечувствительно к регистру.
- **Пользователь** - Текст, соответствующий значению столбца **Пользователь** в просмотрщике журнала аудита. Это поле нечувствительно к регистру.
- **Процесс** - Текст, соответствующий значению столбца **Процесс** в просмотрщике журнала аудита. Это поле нечувствительно к регистру.
- **PID** - Число, соответствующее значению столбца **PID** в просмотрщике журнала аудита. Используя точку с запятой в качестве разделителя, можно задать несколько значений.
- **С** - Начало временного интервала событий для фильтрации. Выберите **Первого события**, чтобы фильтровать события, начиная с самого раннего в журнале. Выберите **События от**, чтобы фильтровать события, произошедшие не ранее определенной даты и времени.
- **По** - Конец временного интервала событий для фильтрации. Выберите **Последнее событие**, чтобы фильтровать события, заканчивая самым поздним в журнале. Выберите **События от**, чтобы фильтровать события, произошедшие не позднее определенной даты и времени.

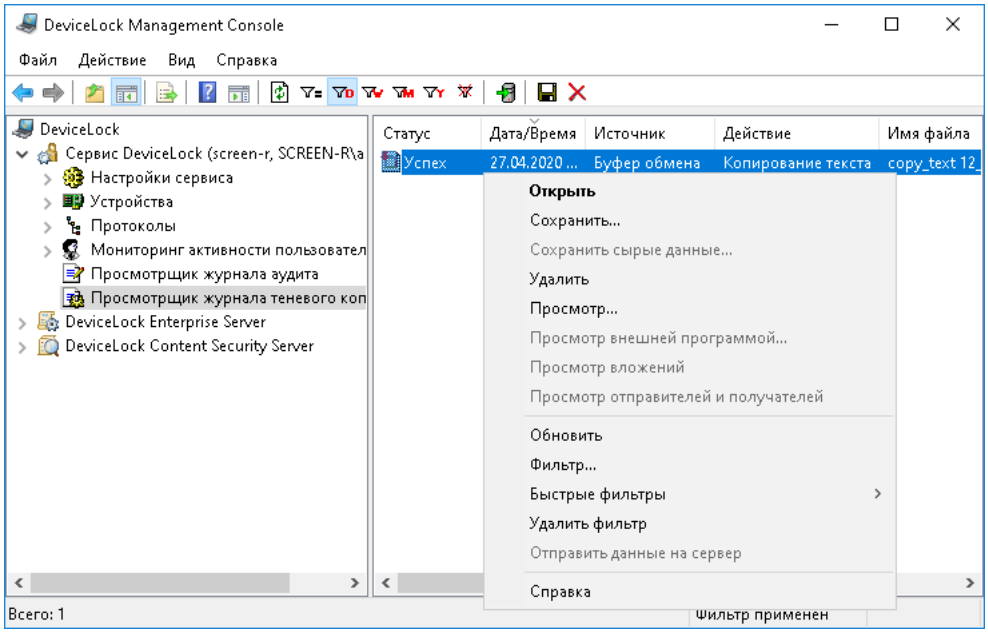
Примечание: Чтобы облегчить настройку фильтра, его строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

Просмотрщик журнала теневого копирования (для компьютера)

Консоль управления содержит встроенный просмотрщик локально сохраненных данных теневого копирования, который позволяет просматривать данные для подключенного компьютера.



Типичная конфигурация DeviceLock подразумевает, что данные теневого копирования хранятся на сервере DeviceLock Enterprise Server. В этом случае данные теневого копирования, полученные и сохраненные сервисом DeviceLock на локальном компьютере, периодически перемещаются на сервер. При этом локальная копия данных теневого копирования удаляется, как только их перемещение на сервер успешно завершается. Для просмотра данных теневого копирования, хранимых на сервере DeviceLock Enterprise Server, используется Просмотрщик журнала теневого копирования (для сервера).

Иногда может быть необходимо просматривать данные теневого копирования, хранящиеся на компьютере пользователя. Такая потребность возникает, например, если сервер DeviceLock Enterprise Server не используется вообще или по каким-то причинам некоторые данные все еще не были перемещены на сервер с компьютеров пользователей.

Столбцы просмотрщика определены следующим образом:

- **Статус** - Состояние записи:
  - **Успех** - Данные успешно запротоколированы.
  - **Неполный** - Данные, возможно, были запротоколированы не полностью.
  - **Отказ** - Устанавливается для теневых копий файлов, передача которых сопровождалась проверкой контентно-зависимыми правилами и была заблокирована на любом из уровней контроля.

  Теневая копия передаваемых данных не создается, если передача данных была запрещена на уровне типа (разрешения для типов устройств), но не проверялась контентно-зависимыми правилами.
- **Дата/Время** - Дата и время передачи данных.
- **Источник** - Тип устройства или протокол.
- **Действие** - Действие пользователя.

- **Имя файла** - Оригинальное имя файла либо автоматически созданное имя для данных, которые изначально не были представлены в виде файла (такие как CD/DVD/BD-образ, данные записанные напрямую на носитель или переданные через COM или LPT-порт)
- **Размер файла** - Размер данных.
- **Тип файла** - Настоящий тип файла.

  Примечание: При применении к файлам, передаваемым на съемные устройства, гибкие диски или оптические носители, данная колонка остается пустой до тех пор, пока устройство или диск не будут извлечены или отключены от системы.

- **Причина** - Указывает, почему произошло событие или чем оно было вызвано. Подробнее см. в описании этого столбца для журнала аудита.
- **Защищен** - Указывает состояние защиты файла. Статус **Да** означает, что файл защищен. Статус **Нет**, равно как и пустой статус, указывает, что защиты на файле нет. Статус **Ошибка** <*текст ошибки*> указывает на ошибку, случившуюся в процессе анализа защиты файла.

  Примечание: Состояние защиты файла может быть получено только на ОС Windows Vista или более новых операционных системах. Попытки получить статус защиты на более старых ОС приводят к следующему сообщению об ошибке в журналах сервера и аудита: “Encryption Analyzer не поддерживается на данной системе”.

- **Информация** - Прочая относящаяся к данному устройству или протоколу информация о событии, такая как флаги доступа, имя устройства или протокола, ID устройства, описание устройства из базы данных (см. База данных USB-устройств) и т.п.
- **Пользователь** - Имя пользователя, передавшего данные.
- **PID** - Идентификатор процесса приложения, использовавшегося для передачи данных.
- **Процесс** - Полный путь к исполняемому файлу приложения. В некоторых случаях вместо полного пути может быть показано только имя процесса.

Управление записями теневого копирования

Для управления записями теневого копирования служит контекстное меню, появляющееся при нажатии правой кнопки мыши на каждой записи. Меню содержит следующие команды:

- Открыть
- Сохранить
- Сохранить сырые данные
- Удалить
- Просмотр
- Просмотр внешней программой
- Просмотр вложений
- Просмотр отправителей и получателей

Открыть

Чтобы открыть файл из выбранной записи в ассоциированном приложении, используйте команду **Открыть** из контекстного меню. Если для этого типа файлов нет ассоциированного приложения, то откроется диалоговое окно **Открыть с помощью**. На пустой записи (размер данных равен 0 или данные не были запротоколированы) команда **Открыть** недоступна.

Чтобы включить шифрование EFS временных файлов, создаваемых при просмотре или открытии теневых копий, добавьте следующее значение реестра:

- Ключ: `HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision`
- Значение: `EncryptTempFiles=dword:00000001`

Допустимые значения: `1`=включено, `0`=выключено. Значение по умолчанию равно `0`.

Сохранить

Если вам необходимо сохранить данные из выбранной записи на локальный компьютер, выберите команду **Сохранить** из контекстного меню или нажмите кнопку на панели инструментов.

Используя клавиши Ctrl и/или Shift, вы можете сохранить данные из нескольких записей одновременно.

Если в записи нет данных (размер данных равен 0 или данные не были запротоколированы), команда **Сохранить** не доступна.

При сохранении большого файла появляется следующее сообщение: “Сохранение файла <путь и имя файла>.” В окне сообщения отображается индикатор выполнения операции. При необходимости операцию сохранения файла можно прервать, нажав кнопку **Отмена**. В этом случае результирующий файл, полученный на локальном компьютере, будет неполным. Этот файл будет содержать только данные, сохраненные до прерывания процесса сохранения.

Данные, которые были переданы пользователем в виде файла, сохраняются в журнале теневого копирования как файл и могут быть сохранены на локальный компьютер тоже как файл.

Когда пользователь записывает данные на CD/DVD/BD-диск, все данные сохраняются в журнале теневого копирования в виде одного образа (один образ на каждый записанный CD/DVD/BD-диск или сессию) в формате CUE.

CD/DVD/BD-образы, а также другие данные, которые изначально не были представлены в виде файлов, показываются в журнале теневого копирования с автоматически созданными именами. Такие имена создаются на основе действия пользователя, имени диска или устройства и даты/времени (например, `direct_write(E:) 19:18:29 17.07.2006.bin`).

Каждый образ CD/DVD/BD сохраняется на локальном компьютере в виде двух файлов - файла данных (например, `direct_write(E_) 19_18_29 17_07_2006.bin`) и файла с расширением .cue, который имеет то же имя, что и файл данных (например, `direct_write(E_) 19_18_29 17_07_2006_bin.cue`). Оба этих файла необходимы для открытия CD/DVD/BD-образа в программах, которые поддерживают формат CUE (такие как Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO и т.п.)

Сохранить сырые данные

Когда вы выбираете запись, которая содержит данные, записанные как дополнительная сессия к уже существующему CD/DVD/BD-диску, в контекстном меню доступен пункт **Сохранить сырые данные**. Эта команда позволяет сохранить данные на локальный компьютер "как есть", без внесения в них каких-либо изменений в процессе сохранения.

Если вы используете обычную функцию сохранения (см. выше), консоль управления может обнаружить, что CD/DVD/BD-образ содержит ссылки на данные из другой (предыдущей) сессии. Поскольку эта предыдущая сессия недоступна (она могла быть записана на диск задолго до того, как сервис DeviceLock был установлен), то консоль управления находит и исправляет все ссылки на эти несуществующие данные, чтобы сделать результирующий файл образа пригодным для чтения в приложениях, поддерживающих формат CUE.

Тем не менее, если вам необходимо получить данные без изменений, то используйте **Сохранить сырые данные**. В этом случае результирующий файл образа может быть не пригодным для чтения в приложениях, поддерживающих формат CUE.

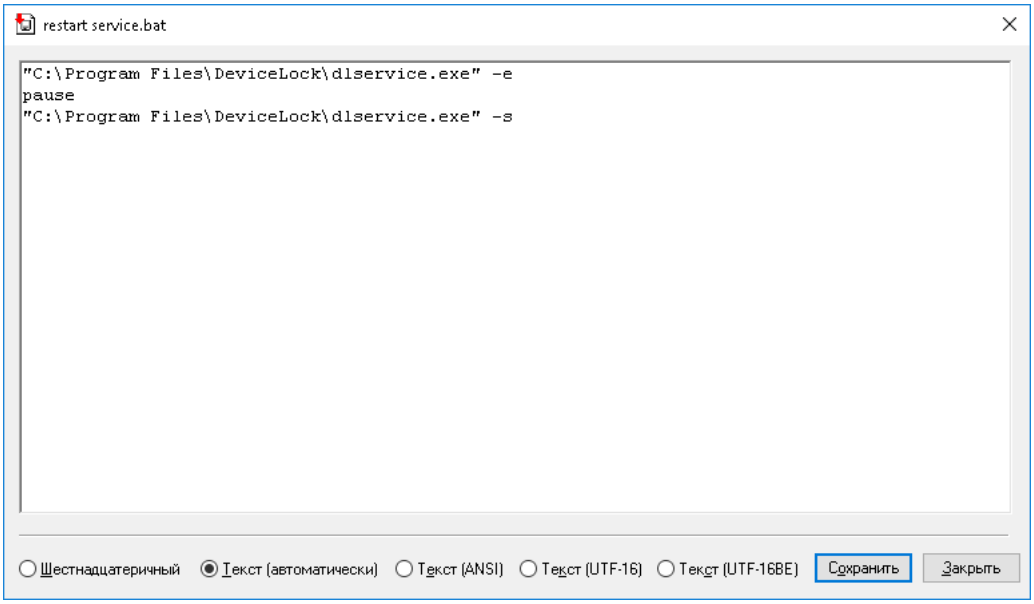
Когда вы сохраняете большой файл, вы можете нажать кнопку **Отмена** на индикаторе выполнения, чтобы прервать сохранение. В этом случае, результирующий файл, который вы получите на локальном компьютере, будет неполным, он будет содержать только те данные, которые были получены до того момента, как вы прервали процесс сохранения.

Удалить ✕

Чтобы удалить запись, используйте команду **Удалить** из контекстного меню или нажмите кнопку ✕ на панели инструментов. Используя клавиши Ctrl и/или Shift, можно выбрать и удалить несколько записей одновременно.

Просмотр

Для просмотра данных в окне встроенного просмотрщика, используйте команду **Просмотр** из контекстного меню.



Предоставляются следующие варианты просмотра:

- **Шестнадцатеричный** - Отображает данные в смешанном (шестнадцатирично-текстовом) формате.
- **Текст (автоматически)** - Автоматически определяет кодировку текста и отображает данные в текстовом формате.
- **Текст (ANSI)** - Задает кодировку текста ANSI и отображает данные в текстовом формате.
- **Текст (UTF-16)** - Задает кодировку текста UTF-16 и отображает данные в текстовом формате.
- **Текст (UTF-16BE)** - Задает кодировку текста UTF-16 с обратным порядком байтов и отображает данные в текстовом формате.

Сохранить данные из просмотрщика во внешний файл можно, нажав кнопку **Сохранить**.

Примечание: Если большой файл открывается для просмотра слишком долго, можно нажать кнопку **Отмена** на индикаторе выполнения, чтобы прервать процесс открытия файла. В этом случае просмотрщик показывает только данные, полученные до того, как процесс открытия был прерван.

Просмотр внешней программой

Также вы можете открыть данные во внешней программе.

Если такая внешняя программа определена, то пункт **Просмотр внешней программой** доступен в контекстном меню. Чтобы задать внешнюю программу просмотра данных, добавьте следующее значение в реестр компьютера, на котором работает консоль управления:

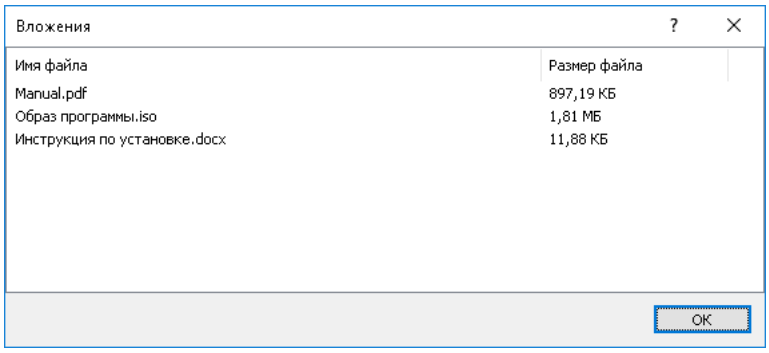
- Ключ: `HKEY_CURRENT_USER\Software\SmartLine Vision\DLManager\Manager`
- Значение: `ExternalShadowViewer=REG_SZ:<полный_путь_к_программе> %1`

Здесь `<полный_путь_к_программе>` - это полный путь к исполняемому файлу программы. Если путь содержит пробелы, то его необходимо заключить в кавычки. Пример: `"C:\Program Files\Microsoft Office\OFFICE11\winword.exe" %1`.

Примечание: Если большой файл открывается для просмотра слишком долго, можно нажать кнопку **Отмена** на индикаторе выполнения, чтобы прервать процесс открытия файла. В этом случае, внешнее приложение отобразит только только данные, полученные до того, как процесс открытия был прерван.

Просмотр вложений

Команда **Просмотр вложений** отображает список вложенных файлов (при их наличии) для теневых eml-копий почтовых сообщений, отправленных/полученных по протоколам SMTP, Web Mail, IBM Notes или MAPI.



Диалоговое окно **Вложения** отображает список вложений со следующими сведениями о каждом файле вложения: имя файла (с расширением) и его размер.

Просматривать вложения можно с помощью просмотрщика данных теневого копирования на клиентском компьютере, просмотрщика данных теневого копирования на сервере DeviceLock Enterprise Server или модуля **Просмотрщик журнала теневого копирования** в консоли DeviceLock Enterprise Manager.

Администраторы сервиса DeviceLock и сервера DeviceLock Enterprise Server, не имеющие доступа к данным теневого копирования, могут использовать команду **Просмотр вложений**, чтобы просматривать список вложений.

Просмотр отправителей и получателей

Команда **Просмотр отправителей и получателей** отображает список отправителей и получателей для теневых копий сообщений, отправленных/полученных по протоколам SMTP, Web Mail, IBM Notes или MAPI. Администраторы сервиса DeviceLock или сервера DeviceLock Enterprise Server, не имеющие прав доступа к содержимому теневых копий, могут использовать эту команду, чтобы выяснить, кто и кому отправил то или иное сообщение.

Управление журналом теневого копирования (для компьютера)

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узел **Сервис DeviceLock** и щелкните правой кнопкой мыши **Просмотрщик журнала теневого копирования** под этим узлом.

  - или -

- В дереве консоли DeviceLock Management Console выберите **Сервис DeviceLock** > **Просмотрщик журнала теневого копирования** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Обновить** - Обновить список записей с учетом последних изменений.
- **Фильтр** - Отображать только записи, удовлетворяющие заданным условиям (см. Фильтр журнала теневого копирования (для компьютера)).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра записей за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

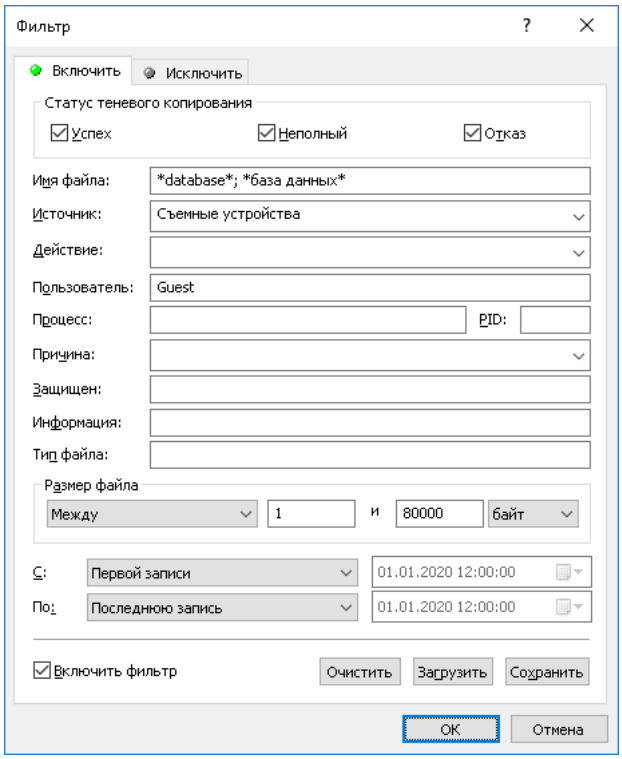
  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).
- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Отправить данные на сервер** - Если в настройках сервиса задан параметр DeviceLock Enterprise Server(ы) и выбрана опция **Включить** или **Только имена файлов** у параметра Отправлять данные теневого копирования на сервер, то для срочной отправки журнала на сервер можно использовать команду **Отправить данные на сервер**. Поскольку сервер DeviceLock Enterprise Server автоматически собирает данные журналов по мере их накопления сервисом DeviceLock, использовать эту команду не обязательно.

Фильтр журнала теневого копирования (для компьютера)

Просмотрщик журнала теневого копирования (для компьютера) позволяет отфильтровать данные так, чтобы в список выводились только записи, удовлетворяющие заданным условиям.

Чтобы открыть диалоговое окно **Фильтр**, выберите команду **Фильтр** из контекстного меню, доступного по нажатию правой кнопки мыши на элементе **Просмотрщик журнала теневого копирования**, или нажмите кнопку ▽= на панели инструментов.



Разница между заданием фильтра для журнала аудита и журнала теневого копирования незначительна, поэтому рекомендуем вначале ознакомится с разделом Фильтр журнала аудита (для компьютера) данного руководства.

Чтобы настроить фильтр, установите флажок **Включить фильтр** на соответствующей вкладке в зависимости от того, следует ли настраивать условия включения или исключения.

Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

Когда фильтр включен, можно определить условия фильтрации, задав необходимые значения в следующих полях:

- **Успех** - Флажок, определяющий нужно ли фильтровать успешно запротоколированные данные.
- **Неполный** - Флажок, определяющий, нужно ли фильтровать данные, которые возможно были запротоколированы не полностью.
- **Отказ** - Флажок, определяющий необходимость фильтровать запротоколированные данные, передача которых сопровождалась проверкой контентно-зависимыми правилами и была заблокирована на любом из уровней контроля.
- **Имя файла** - Текст, соответствующий значению столбца **Имя файла** в просмотрщике журнала теневого копирования. Это поле нечувствительно к регистру.
- **Источник** - Выбираемый параметр, соответствующий значению столбца **Источник** в просмотрщике журнала теневого копирования. Это поле нечувствительно к регистру.

- **Действие** - Выбираемый параметр, соответствующий значению столбца **Действие** в просмотрщике журнала теневого копирования. Это поле нечувствительно к регистру.
- **Пользователь** - Текст, соответствующий значению столбца **Пользователь** в просмотрщике журнала теневого копирования. Это поле нечувствительно к регистру.
- **Процесс** - Текст, соответствующий значению столбца **Процесс** в просмотрщике журнала теневого копирования. Это поле нечувствительно к регистру.
- **PID** - Число, соответствующее значению столбца **PID** в просмотрщике журнала теневого копирования. Используя точку с запятой в качестве разделителя, можно задать несколько значений.
- **Причина** - Текст, соответствующий значению столбца **Причина** в просмотрщике журнала теневого копирования. Это поле нечувствительно к регистру.
- **Защищен** - Текст, соответствующий значению столбца **Защищен** в просмотрщике журнала теневого копирования.
- **Информация** - Текст, соответствующий значению столбца **Информация** в просмотрщике журнала теневого копирования. Это поле нечувствительно к регистру.
- **Тип файла** - Текст, соответствующий значению столбца **Тип файла** в просмотрщике журнала теневого копирования. Это поле нечувствительно к регистру.
- **Размер файла** - Число или интервал чисел, соответствующих значению столбца **Размер файла** в просмотрщике журнала теневого копирования.
- **С** - Начало временного интервала записей для фильтрации. Выберите **Первой записи,** чтобы фильтровать записи, начиная с самой ранней в журнале. Выберите **Записи от**, чтобы фильтровать записи, выполненные не ранее определенной даты и времени.
- **По** - Конец временного интервала записей для фильтрации. Выберите **Последнюю запись**, чтобы фильтровать записи, заканчивая самой поздней в журнале. Выберите **Записи от**, чтобы фильтровать записи, выполненные не позднее определенной даты и времени.

Примечание: Чтобы облегчить настройку фильтра, его строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

Управление сервисом DeviceLock для Mac

Управление сервисом DeviceLock для Mac может выполняться из консоли DeviceLock Management Console точно так же, как и управление сервисом DeviceLock для Windows (см. раздел Управление сервисом DeviceLock для Windows).

Примечание: Для удаленного управления различными экземплярами сервиса DeviceLock для Mac из консолей управления DeviceLock с использованием локальных учетных записей для компьютеров, на которых установлен сервис DeviceLock для Mac, системная опция **Предоставление общего доступа к файлам и папкам с помощью SMB** должна быть включена для этих локальных учетных записей или должно быть разрешено хеширование NTLM для этих локальных учетных записей. Для более подробной информации обратитесь к разделу Разрешение NTLM-аутентификации для локальных пользователей в Mac OS X.

В отличие от сервиса DeviceLock для Windows, сервис DeviceLock для Mac поддерживает только следующие параметры и настройки:

Настройки сервиса

- Администраторы DeviceLock (не поддерживаются параметры: "Включить защиту от отключения", "Предотвращать изменения в системных файлах настроек", "Использовать усиленную проверку целостности")
- DeviceLock Enterprise Server(ы)
- Сертификат DeviceLock
- Использовать групповые/серверные политики
- Быстрые серверы вначале
- Способ определения режима офлайн
- Подавлять локальную политику
- Записывать события об изменении политики и старте/остановке сервиса

Настройки сервиса > Аудит и теневое копирование

- Отправлять данные теневого копирования на сервер

Настройки сервиса > Шифрование

- Mac OS X FileVault

Устройства

- Bluetooth (разрешения, аудит)
- FireWire-порт (разрешения, аудит)
- Жесткий диск (разрешения, аудит)
- Оптический привод (разрешения, аудит)
- Съемные устройства (разрешения, аудит, теневое копирование)
- Последовательный порт (разрешения, аудит)
- USB-порт (разрешения, аудит)
- WiFi (разрешения, аудит)
- Белый список USB-устройств (единственный поддерживаемый флаг - "Контролировать как тип")
- Белый список носителей

Примечание: Права доступа для типа устройств Bluetooth не применяются к Bluetooth-устройствам ввода (мышь, клавиатура и т.д.). Это сделано для предотвращения блокирования беспроводных клавиатуры и мыши на iMac и Mac Pro.

Настройки безопасности

- Управлять доступом к USB HID
- Управлять доступом к USB Bluetooth-адаптерам
- Управлять доступом к сетевым картам USB и FireWire
- Управлять доступом к устройствам хранения USB
- Управлять доступом к устройствам хранения FireWire

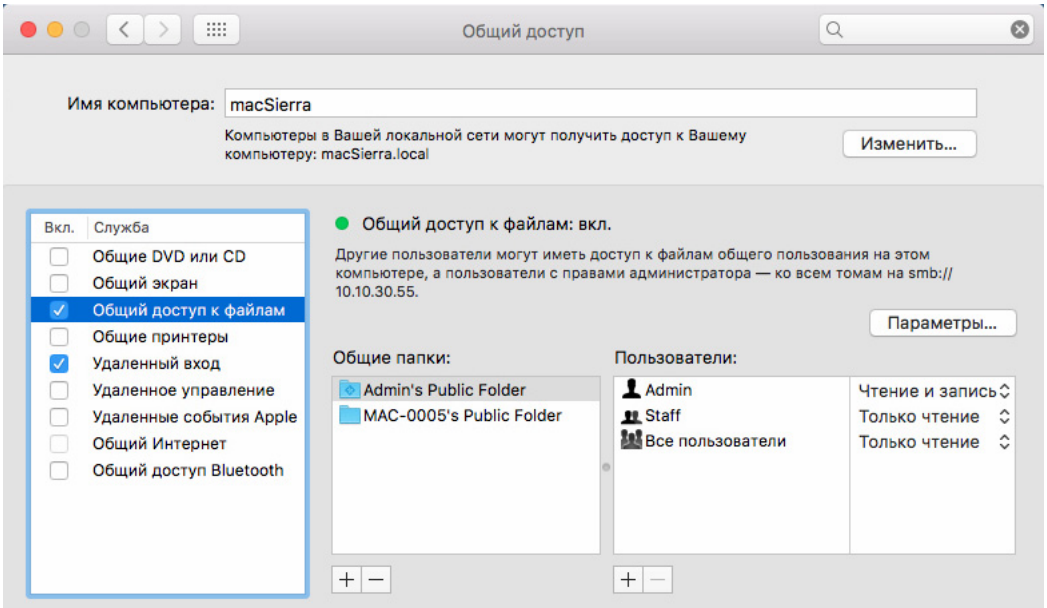
Разрешение NTLM-аутентификации для локальных пользователей в Mac OS X

Для безопасного сетевого соединения с другими компонентами DeviceLock сервис DeviceLock для Mac использует NTLM-аутентификацию и шифрование. Эти механизмы работают по умолчанию, если компьютер Mac введен в домен Active Directory. NTLM-аутентификация локальных пользователей как правило запрещена. Чтобы использовать консоли DeviceLock для управления компьютерами Mac вне домена Active Directory, NTLM-аутентификация ДОЛЖНА быть разрешена для локального пользователя.

Существует два способа разрешения NTLM для локальных пользователей в Mac:

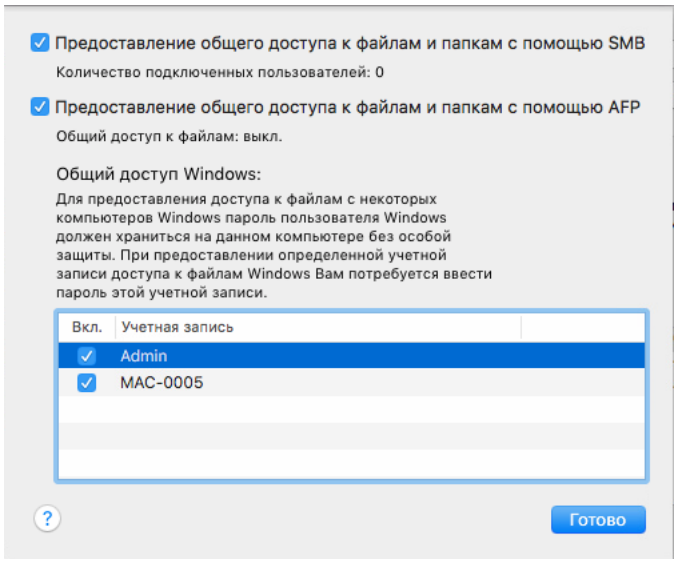
1. **Дружественный для пользователя способ.** Подходит для Mac OS X версии 10.7 и выше. Способ для операционных систем версии 10.6 см. далее в этом разделе.

   a) Откройте панель **Общий доступ** в системных настройках компьютера, затем выберите пункт **Общий доступ к файлам**.



   b) Нажмите кнопку **Параметры**.

Появится диалоговое окно со списком всех локальных пользователей. Флажок **Предоставление общего доступа к файлам и папкам с помощью SMB** в этом диалоговом окне включает поддержку NTLM-аутентификации для каждого пользователя, выбранного в списке.

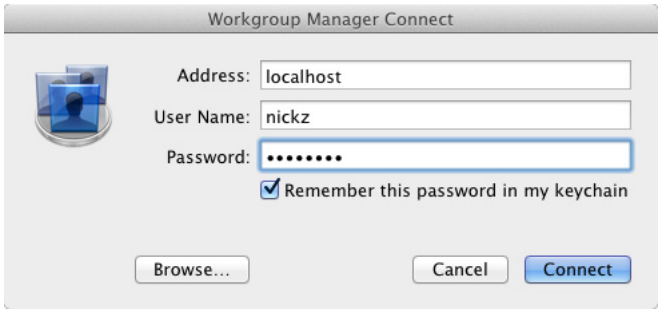


2. **Альтернативный способ.** Подходит для операционных систем Mac OS X 10.6, 10.7 и выше.

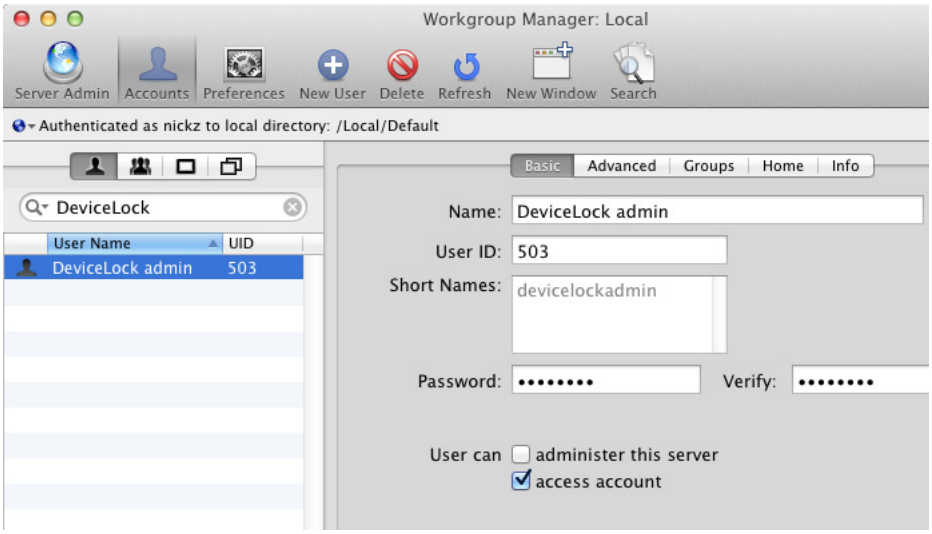
   a) Установите Server Admin Tools:

      - Server Admin Tools 10.6.8 http://support.apple.com/kb/HT3931
      - Server Admin Tools 10.7.3 http://support.apple.com/kb/HT202366

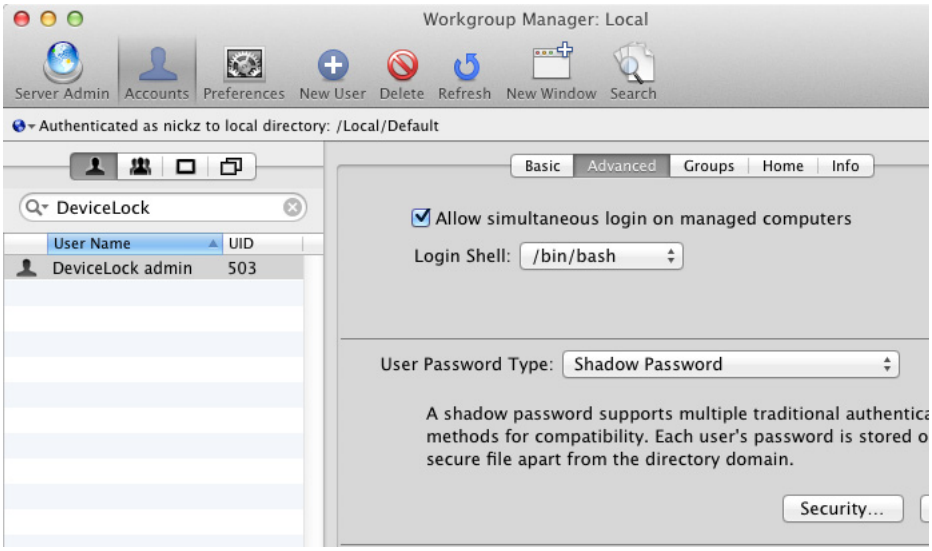
   b) Запустите Workgroup Manager из Server Admin Tools. Укажите имя компьютера, к которому следует подключиться, и учетную запись с правами администратора.



c) После аутентификации появится основное окно. Выберите пользователя из списка слева.

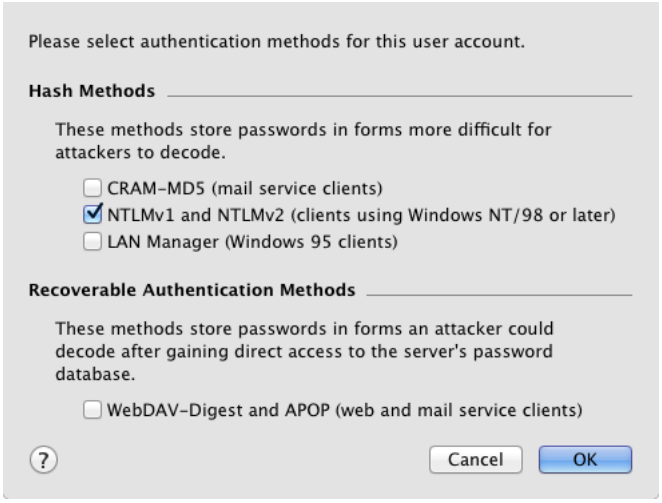


d) Откройте вкладку **Advanced**.



e) Нажмите кнопку **Security**.

f) Установите флажок **NTLMv1 and NTLMv2**, затем примените изменения. Наконец, измените пароль для пользователя, которому была разрешена NTLM-аутентификация.



Примечание:

- NTLM-аутентификация будет недоступна, пока пароль пользователя не будет изменен. Это следствие ограничений базы данных паролей в Mac OS X. При этом не требуется, чтобы новый пароль отличался от старого.
- Поддержка NTLM-аутентификации включается индивидуально для каждого пользователя.

5

Контентно-зависимые правила (обычный профиль)

В этой главе:

Правила для устройств

Правила для протоколов

Настройка контентных групп

Управление контентно-зависимыми правилами

Правила для устройств

Контентно-зависимые правила для устройств расширяют базовую функциональность контроля доступа к портам и устройствам в DeviceLock DLP, обеспечивая высокотехнологичный уровень защиты конфиденциальных документов организации посредством использования технологий контентного анализа и фильтрации содержимого файлов и данных. Они обеспечивают автоматическую проверку содержимого данных, копируемых на внешние устройства хранения данных, обнаружение конфиденциальных данных и применение необходимых политик безопасности.

Контентно-зависимые правила позволяют избирательно разрешать или блокировать доступ к специфичному содержимому файлов и данных независимо от разрешений, установленных на уровне типа устройства. Кроме того, контентно-зависимые правила могут быть использованы для избирательного теневого копирования на основании анализа содержимого, или для обнаружения попыток чтения, записи или удаления файлов с определенным содержимым без блокирования доступа и без создания теневых копий. Правила можно задавать применительно к тем или иным типам устройств индивидуально для различных пользователей и/или групп.

Контентно-зависимые правила могут быть заданы для операций контроля доступа, теневого копирования, обнаружения содержимого, или для любой комбинации этих операций.

Следующие примеры демонстрируют использование контентно-зависимых правил.

- **Пример 1 - Использование контентно-зависимых правил для операций контроля доступа**. Можно разрешить отдельным пользователям или группам чтение документов, содержащих выражение “Для служебного пользования”, со съемных устройств, гибких дисков и оптических дисков, но запретить им запись файлов, содержащих более одного номера кредитной карты, на съемные устройства и гибкие диски.
- **Пример 2 - Использование контентно-зависимых правил для операций теневого копирования**. Для проведения аудита информационной безопасности и в целях расследования инцидентов информационной безопасности можно указать, что теневые копии будут созданы только для файлов, содержащих номера кредитных карт, номера СНИЛС, а также выражения “Совершенно секретно” и “Для служебного пользования”.
- **Пример 3 - Использование контентно-зависимых правил для операций обнаружения содержимого.** Можно задать правило, предусматривающее журналирование и отправку тревожного оповещения при попытках передачи файлов размером свыше 20 МБ, без блокирования передачи или создания теневых копий таких файлов.

Контентно-зависимые правила могут применяться к следующим типам устройств: Буфер обмена, Гибкий диск, iPhone-устройства, MTP, Оптический привод, Palm, Принтер, Съемные устройства, TC-устройства и Windows Mobile.

Примечание: При определении контентно-зависимых правил для принтеров учитывайте следующее:

- Сервис DeviceLock может выполнить анализ содержимого печатаемых документов, только если на вкладке **Дополнительно** диалогового окна **Свойства** для принтера выбраны параметры **Использовать очередь печати (ускорение работы приложений)** и **Начинать печать после помещения в очередь всего задания**.
- К документам, отправляемым на печать, не применяются контентные группы Определение типа файла, а также следующие параметры контентных групп Свойства документа и Цифровые отпечатки: **Размер, Изменен, Имя файла, Доступ от процесса, Защищен паролем, Содержит текст, Дополнительные параметры, Точное совпадение файла, Использовать только бинарные отпечатки для файлов, защищенных паролем.**

Узел “Контентно-зависимые правила”

Под узлом **Устройства** > **Контентно-зависимые правила** в дереве консоли перечисляются пользователи и группы, для которых заданы контентно-зависимые правила, относящиеся к устройствам. Контентно-зависимые правила могут быть заданы индивидуально для каждого пользователя и группы применительно к тем или иным типам устройств.

Примечание: Можно задавать различные контентно-зависимые правила для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Контентно-зависимые правила для оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Контентно-зависимые правила для автономного режима (офлайн-профиль) применяются, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Описание политик DeviceLock для автономного режима можно найти в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по настройке контентно-зависимых правил см. в разделе Управление контентно-зависимыми правилами для автономного режима.

Контекстное меню узла **Контентно-зависимые правила** содержит следующие команды:

- **Управление** - Открывает диалоговое окно, позволяющее задать или отредактировать контентно-зависимые правила для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее задать или отредактировать контентно-зависимые правила для автономного режима.
- **Загрузить** - Позволяет импортировать ранее сохраненный файл с контентно-зависимыми правилами для оперативного режима.
- **Загрузить офлайновые настройки** - Позволяет импортировать ранее сохраненный файл с контентно-зависимыми правилами для автономного режима.
- **Сохранить** - Позволяет экспортировать контентно-зависимые правила, заданные для оперативного режима, в файл с расширением .cwl, который затем можно импортировать и использовать на другом компьютере.
- **Сохранить офлайновые настройки** - Позволяет экспортировать контентно-зависимые правила, заданные для автономного режима, в файл с расширением .cwl, который затем можно импортировать и использовать на другом компьютере.
- **Сбросить** - Сбрасывает контентно-зависимые правила для оперативного режима в состояние “не задано”. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

- **Сбросить офлайновые настройки** - Сбрасывает контентно-зависимые правила для автономного режима в состояние “не задано”. Если такие правила не заданы, к клиентским компьютерам, находящимся не в сети, применяются правила, заданные для оперативного режима.
- **Удалить офлайновые настройки** - Блокирует наследование контентно-зависимых правил, заданных для автономного режима, и принудительно применяет правила, заданные для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

Пользователи и группы, для которых заданы контентно-зависимые правила, отображаются под узлом **Контентно-зависимые правила** в дереве консоли и имеют такое же контекстное меню, что и этот узел, за исключением команды **Сбросить офлайновые настройки** и с добавлением команды **Удалить пользователя**, которая удаляет контентно-зависимые правила для выбранного пользователя или группы.

Подробнее см. в разделах:

Настройка контентных групп

Управление контентно-зависимыми правилами

Список контентно-зависимых правил для устройств

Пользователи и группы, для которых заданы контентно-зависимые правила, относящиеся к устройствам, отображаются под узлом **Устройства** > **Контентно-зависимые правила** в дереве консоли (подробнее см. в разделе Узел “Контентно-зависимые правила”).

Если выбрать пользователя или группу под узлом **Контентно-зависимые правила** в дереве консоли, на панели сведений отображаются контентно-зависимые правила, заданные для этого пользователя или группы. Для каждого правила список содержит следующие сведения:

- **Имя** - Имя правила. По умолчанию контентно-зависимое правило имеет то же имя, что и указанная в правиле контентная группа.
- **Тип** - Тип анализа содержимого файла. Возможные значения:
  - **Определение типа файла** - Означает, что идентификация файлов ведется по сигнатурам.
  - **Ключевые слова -** Означает, что идентификация данных/файлов ведется по заданным ключевым словам и выражениям.
  - **Шаблон** означает, что идентификация данных/файлов ведется на основе заданных шаблонов регулярных выражений Perl.
  - **Свойства документа -** Означает, что идентификация файлов ведется по их свойствам.
  - **Цифровые отпечатки** - Означает, что идентификация файлов ведется по их цифровым отпечаткам.
  - **Составное -** Означает, что идентификация данных/файлов ведется по заданному контенту, описанному логическим выражением.
- **Действие** - Показывает, какие действия с файлами пользователю разрешены или запрещены, а также какие действия пользователя будут записываться в журнале теневого копирования.

- **Применяется к** - Возможные значения:
  - **Разрешения** - Означает, что правило применяется для операций контроля доступа.
  - **Теневое копирование** - Означает, что правило применяется к операциям избирательного теневого копирования.
  - **Обнаружение -** Означает, что правило применяется к операциям обнаружения.
  - **Разрешения+Теневое копирование** - Означает, что правило применяется к операциям контроля доступа и операциям избирательного теневого копирования.
  - **Разрешения+Обнаружение** - Означает, что правило применяется к операциям контроля доступа и операциям обнаружения.
  - **Теневое копирование+Обнаружение** - Означает, что правило применяется к операциям избирательного теневого копирования и операциям обнаружения.
  - **Разрешения+Теневое копирование+Обнаружение** - Означает, что правило применяется ко всем возможным видам операций: контроля доступа, избирательного теневого копирования и обнаружения содержимого.
- **Тип устройства** - Тип(ы) устройств, к которым применяется правило.
- **Отправить алерт** - Отображает, включены ли тревожные оповещения для данного правила.
- **Протоколировать событие** - Отображает, включена ли регистрация событий в журнале аудита для данного правила.
- **Теневое копирование** - Отображает, будет ли создана теневая копия в результате срабатывания данного правила.
- **Профиль** - Возможные значения: **Обычный** и **Офлайн**. Значение **Обычный** указывает, что правило применяется к компьютерам, находящимся в сети. Значение **Офлайн** указывает, что правило применяется к компьютерам, работающим автономно.

  Одним и тем же пользователям или группам можно задавать разные правила для разных профилей. О работе с правилами офлайн-профиля см. в разделе Управление контентно-зависимыми правилами для устройств в автономном режиме.

Контекстное меню правила в списке на панели сведений содержит следующие команды:

- **Управление** - В зависимости от профиля данного правила (обычный или офлайн), открывает диалоговое окно, в котором можно задать контентно-зависимые правила для оперативного или автономного режима.
- **Редактировать** - Открывает диалоговое окно, в котором можно просмотреть или изменить данное правило.
- **Отправить алерт** - Включает или отключает отправку оповещений для данного правила.
- **Протоколировать событие** - Включает или отключает протоколирование событий для данного правила.
- **Теневое копирование** - Включает или отключает теневое копирование контента, вызывающего срабатывание данного правила.
- **Удалить** - Удаляет данное правило.

Подробнее см. в разделе Управление контентно-зависимыми правилами.

Управление доступом к контенту

Когда контентно-зависимые правила применяются к операциям контроля доступа, они контролируют операции чтения, записи и удаления определенного контента. Операции удаления и записи контролируются совместно при помощи права на запись.

Контентно-зависимые правила для устройств позволяют:

- Предоставить доступ на чтение/запись для указанного содержимого файлов, когда доступ запрещен на уровне типа устройства.
- Запретить доступ на чтение/запись для указанного содержимого файлов, когда доступ разрешен на уровне типа устройства.

Примечание: DeviceLock может проверять доступ к устройствам на двух уровнях: на уровне интерфейса (порта) и на уровне типа устройства. Некоторые устройства проверяются на обоих уровнях, другие проверяются только на одном уровне - интерфейса (порта) или типа устройства. Например, USB-устройства флэш-памяти проверяются на обоих уровнях: интерфейса (**USB-порт**) и типа устройства (**Съемные устройства**). Контентно-зависимые правила применяются только при условии, что проверка доступа проводится на уровне типа устройства (**Съемные устройства**, **Гибкие диски**, и т.д.). DeviceLock не проводит проверку доступа для USB устройств на уровне типа устройства, если выполняются следующие условия:

- Устройство отсутствует в белом списке USB-устройств, параметр **Управлять доступом к устройствам хранения USB** включен в настройках безопасности, и у пользователя нет доступа к устройствам типа **USB-порт**.

  - или -
- Устройство присутствует в белом списке USB-устройств и флажок **Контролировать как тип** для него не установлен.

Следующая таблица содержит сведения о правах доступа, которые используются при создании контентно-зависимых правил.

Права доступа	Описание
Основные: Чтение	Право на чтение файлов с указанным содержимым с устройства. Применимо только к типам **Оптический привод**, **Гибкий диск** и **Съемные устройства**.
Основные: Запись	Право на запись файлов с указанным содержимым на устройство. Применимо только к типам **Гибкий диск** и **Съемные устройства**.
Основные: Чтение, Запись	Право на чтение и запись файлов с указанным содержимым с/на устройство. Данное право применимо только к типам **Гибкий диск** и **Съемные устройства**.
Основные: Печать	Право на печать документов с указанным содержимым. Применимо только к типу **Принтер**.
Основные: Чтение с подключенного диска	Право на чтение данных с указанным содержимым с подключенного диска в терминальной сессии. Применимо только к типу **ТС-устройства**.
Основные: Запись на подключенный диск	Право на запись данных с указанным содержимым на подключенный диск в терминальной сессии. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена входящий текст	Право на вставку текстовых данных с указанным содержимым из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена входящие файлы	Право на вставку файлов с указанным содержимым из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.

Права доступа	Описание
Основные: Буфер обмена входящие изображения	Право на вставку изображений с указанным содержимым из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена входящие неизвестные данные	Право на вставку прочих данных с указанным содержимым из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена исходящий текст	Право на вставку текстовых данных с указанным содержимым из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена исходящие файлы	Право на вставку файлов с указанным содержимым из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена исходящие изображения	Право на вставку изображений с указанным содержимым из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена исходящие неизвестные данные	Право на вставку прочих данных с указанным содержимым из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Зашифрованные: Чтение	Право на чтение файлов с указанным содержимым с зашифрованного устройства, поддерживаемого сервисом DeviceLock. Применимо только к типу **Съемные устройства**.
Зашифрованные: Запись	Право на запись файлов с указанным содержимым на зашифрованное устройство, поддерживаемое сервисом DeviceLock. Применимо только к типу **Съемные устройства**.
Зашифрованные: Чтение, Запись	Право на чтение и запись файлов с указанным содержимым с/на зашифрованное устройство, поддерживаемое сервисом DeviceLock. Применимо только к типу **Съемные устройства**.
Специальные разрешения: Копирование текста	Право на вставку текстовых данных с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование неидентифицированного содержимого	Право на вставку прочих данных с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование файла	Право на вставку файлов с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование изображения	Право на вставку изображений с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование экрана	Право на вставку снимков экрана с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.

Примечание: Права доступа **Основные**, установленные для съемных устройств, применяются только к не зашифрованным устройствам. Права доступа **Зашифрованные**, установленные для съемных устройств, применяются только к зашифрованным устройствам. Чтобы установить права доступа одновременно для зашифрованных и не зашифрованных съемных устройств, необходимо одновременно задать права доступа **Основные** и **Зашифрованные**. Перечень устройств, распознаваемых сервисом DeviceLock как зашифрованные, см. в разделе Шифрование.

Следующая таблица показывает, как разрешения, предоставленные на разных уровнях, влияют на права доступа пользователя. Разрешения на уровне типа - это разрешения, заданные для типа устройств. Разрешения на уровне файла - это разрешения, заданные при помощи контентно-зависимых правил.

	Полный доступ на уровне типа	**Нет доступа** на уровне типа	**Чтение разрешено** **Запись запрещена** на уровне типа
Чтение разрешено на уровне файла	Разрешает чтение любого содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение любого содержимого, кроме заданного. Запрещает создание, переименование и удаление и пустых папок и файлов нулевого размера.	Разрешает чтение любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера
Чтение запрещено на уровне файла	Запрещает чтение заданного содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение и запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение заданного содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.
Запись разрешена на уровне файла	Разрешает запись любого содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает запись любого содержимого, кроме заданного. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает запись любого содержимого, кроме заданного. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.
Запись запрещена на уровне файла	Запрещает запись заданного содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение и запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.

	Полный доступ на уровне типа	**Нет доступа** на уровне типа	**Чтение разрешено** **Запись запрещена** на уровне типа
Чтение разрешено **Запись разрешена** на уровне файла	Разрешает чтение и запись любого содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение и запись любого содержимого, кроме заданного. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Разрешает чтение любого содержимого. Запрещает запись любого содержимого, кроме заданного. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.
Чтение запрещено **Запись запрещена** на уровне файла	Запрещает чтение и запись заданного содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение и запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение заданного содержимого. Запрещает запись любого содержимого; Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.
Чтение разрешено **Запись запрещена** на уровне файла	Разрешает чтение любого содержимого. Запрещает запись заданного содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение любого содержимого, кроме заданного. Запрещает запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.	Разрешает чтение любого содержимого. Запрещает запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.
Чтение запрещено **Запись разрешена** на уровне файла	Запрещает чтение заданного содержимого. Разрешает запись любого содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение любого содержимого. Запрещает запись любого содержимого, кроме заданного. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение заданного содержимого. Запрещает запись любого содержимого, кроме заданного. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.

	Полный доступ на уровне типа	**Нет доступа** на уровне типа	**Чтение разрешено** **Запись запрещена** на уровне типа
Теневое копирование: Разрешено / Запрещено на уровне файла	Разрешает чтение и запись любого содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение и запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.	Разрешает чтение любого содержимого. Запрещает запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.
Обнаружение: Чтение разрешено / Запись разрешена на уровне файла	Разрешает чтение и запись любого содержимого. Разрешает создание, переименование и удаление пустых папок и файлов нулевого размера.	Запрещает чтение и запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.	Разрешает чтение любого содержимого. Запрещает запись любого содержимого. Запрещает создание, переименование и удаление пустых папок и файлов нулевого размера.

Примечание: Если для типа устройства не установлено никаких разрешений (доступ запрещен), и при этом задано контентно-зависимое правило, разрешающее запись содержимого или обнаружение содержимого для этого типа устройств, пользователь получает право на обзор папок. Разрешение на обзор папок позволяет перемещаться по папкам и просматривать списки файлов и подпапок, даже если пользователь не имеет разрешения на чтение просматриваемых файлов и папок.

При использовании контентно-зависимых правил необходимо учитывать следующее:

- Запрещающие контентно-зависимые правила имеют приоритет перед разрешающими правилами, если правила применяются для одного и того же пользователя или групп пользователей.

  Исключение: разрешающее контентно-зависимое правило на основе группы свойств документа с выбранной опцией **Извлечение текста не поддерживается** имеет приоритет над запрещающими правилами, позволяя передавать любой подходящий под это правило контент, в том числе части многотомных архивов.

  Исключение: разрешающее контентно-зависимое правило на основе группы свойств документа с выбранной опцией **Защищено паролем** имеет приоритет над запрещающими правилами, позволяя передавать любой подходящий под это правило контент. Разрешающее комплексное правило будет иметь приоритет только в том случае, если в числе групп разрешающей логической цепочки, с которыми совпал файл, будет группа свойств документа с выбранной опцией **Защищено паролем**.

  Исключение: разрешающее контентно-зависимое правило на основе группы цифровых отпечатков с выбранной опцией **Точное совпадение файла** имеет приоритет над запрещающими правилами, позволяя передавать любой подходящий под это правило контент. Разрешающее комплексное правило будет иметь приоритет только в том случае, если в числе групп разрешающей логической цепочки, с которыми совпал файл, будет группа цифровых отпечатков с выбранной опцией **Точное совпадение файла**.

- Разрешающие контентно-зависимые правила разрешают передачу целиком всего объекта данных (сообщения или файла, включая архивы и контейнеры), если в нем присутствует содержимое, удовлетворяющее этим правилам и отсутствует содержимое, явно запрещенное запрещающими контентно-зависимыми правилами.

- Когда пользователь пытается перезаписать существующий файл, не имея разрешения на запись нового файла, старый файл будет удален. Для предотвращения такого поведения включите параметр Безопасная перезапись файла в узле консоли Настройки сервиса.
- Когда пользователь пытается изменить файл, не имея разрешения на запись, файл будет удален. Для предотвращения такого поведения задайте параметр Безопасная перезапись файла в узле консоли Настройки сервиса.
- Когда пользователь открывает файл для его модификации посредством вставки запрещенного содержимого, а затем пытается его сохранить, файл будет удален. Для предотвращения такого поведения задайте параметр Безопасная перезапись файла в узле консоли Настройки сервиса.
- Небезопасное извлечение устройства может привести к повреждению данных и файловой системы устройства.
- Когда пользователь пытается копировать файлы, не имея разрешения на запись, файлы временно отображаются в проводнике Windows и других файловых менеджерах. В действительности этих файлов нет на конечном устройстве, они находятся в кэше памяти и будут удалены из кэша сразу после того, как DeviceLock закончит проверку их содержимого.
- Проверка содержимого файлов может отнимать много времени. До тех пор, пока проверка не будет завершена, невозможно безопасно извлечь устройство, даже если файлы отображаются в проводнике Windows или других файловых менеджерах. В этой ситуации выводится сообщение об ошибке, указывающее, что устройство занято.
- Недавно скопированные файлы нельзя будет открыть для чтения до тех пор, пока DeviceLock не закончит проверку их содержимого.
- Проверка содержимого файлов может отнимать много времени. Можно указать сообщение о проверке содержимого, которое будет отображаться пользователям во время проверки. Подробнее об этом сообщении см. в описании параметра Сообщение о проверке содержимого.
- Когда пользователь пытается прочитать или записать содержимое файлов, не имея разрешения на чтение и запись, выводится сообщение о блокировании чтения или сообщение о блокировании записи, если включен соответствующий параметр в настройках сервиса DeviceLock (см. описание параметров Контентно-зависимое сообщение о блокировании чтения и Контентно-зависимое сообщение о блокировании записи).

Теневое копирование контента

Прежде чем можно будет использовать контентно-зависимые правила для операций теневого копирования, необходимо включить теневое копирование на уровне типа устройства. Контентно-зависимые правила, применяемые к операциям теневого копирования, позволяют фильтровать теневые копии данных и файлов, записываемых пользователями. Использование контентно-зависимых правил в дополнение к настройке теневого копирования на уровне типа устройств позволяет существенно снизить объем копируемых данных, обеспечивая теневое копирование только таких файлов, содержимое которых существенно для информационной безопасности.

Следующая таблица содержит сведения о правах теневого копирования, которые используются при создании контентно-зависимых правил.

Право теневого копирования	Описание
Основные: Чтение	Определяет, создается ли теневая копия данных с указанным содержимым, считываемых с устройства. Применимо только к типу **MTP**.
Основные: Запись	Определяет, создается ли теневая копия данных с указанным содержимым, записываемых на устройство. Применимо к типам **Гибкий диск**, **iPhone-устройства**, **MTP**, **Съемные устройства**, **Palm** и **Windows Mobile**.
Основные: Запись на подключенный диск	Определяет, создается ли теневая копия данных с указанным содержимым, записываемых на устройство. Применимо только к типу **TC-устройства**.
Основные: Печать	Определяет, создается ли теневая копия документов с указанным содержимым, посылаемых на принтер. Применимо только к типу **Принтер**.
Основные: Копирование в буфер обмена	Определяет, создается ли теневая копия данных с указанным содержимым, вставляемых из буфера обмена. Применимо только к типу **Буфер обмена**.
Основные: Буфер обмена входящий текст	Определяет, создается ли теневая копия текстовых данных с указанным содержимым, вставляемых из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **TC-устройства**.
Основные: Буфер обмена исходящий текст	Определяет, создается ли теневая копия текстовых данных с указанным содержимым, вставляемых из буфера обмена окна терминальной сессии /виртуальной машины. Применимо только к типу **TC-устройства**.
Основные: Буфер обмена входящие изображения	Определяет, создается ли теневая копия изображений с указанным содержимым, вставляемых из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **TC-устройства**.
Основные: Буфер обмена исходящие изображения	Определяет, создается ли теневая копия изображений с указанным содержимым, вставляемых из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу **TC-устройства**.
Основные: Буфер обмена входящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым, вставляемых из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **TC-устройства**.

Право теневого копирования	Описание
Основные: Буфер обмена исходящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым, вставляемых из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена входящие неизвестные данные	Определяет, создается ли теневая копия прочих данных с указанным содержимым, вставляемых из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена исходящие неизвестные данные	Определяет, создается ли теневая копия прочих данных с указанным содержимым, вставляемых из буфера обмена окна терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Зашифрованные: Запись	Определяет, создается ли теневая копия данных с указанным содержимым, записываемых на зашифрованное устройство. Применимо только к типу **Съемные устройства**.
Специальные разрешения: Запись календаря	Определяет, создается ли теневая копия календарей с указанным содержимым, записываемых на мобильное устройство. Применимо к типам **iPhone-устройства**, **Palm** и **Windows Mobile**.
Специальные разрешения: Запись контакта	Определяет, создается ли теневая копия контактов с указанным содержимым, записываемых на мобильное устройство. Применимо к типам **iPhone-устройства**, **Palm** и **Windows Mobile**.
Специальные разрешения: Запись электронной почты	Определяет, создается ли теневая копия сообщений электронной почты с указанным содержимым, записываемых на мобильное устройство. Применимо к типам **iPhone-устройства**, **Palm** и **Windows Mobile**. Для iPhone-устройств это право контролирует теневое копирование настроек учетной записи электронной почты, но не сообщений, так как приложение iTunes не поддерживает синхронизацию сообщений.
Специальные разрешения: Запись вложения	Определяет, создается ли теневая копия вложений электронной почты с указанным содержимым, записываемых на устройство типа **Windows Mobile** или **Palm**.
Специальные разрешения: Запись избранного	Определяет, создается ли теневая копия закладок с указанным содержимым, записываемых на устройство типа **Windows Mobile** или **iPhone-устройства**.
Специальные разрешения: Запись файла	Определяет, создается ли теневая копия файлов с указанным содержимым, записываемых на мобильное устройство. Применимо к типам **iPhone-устройства**, **Palm** и **Windows Mobile**.
Специальные разрешения: Запись медиа-данных	Определяет, создается ли теневая копия медиа-данных с указанным содержимым, записываемых на устройства типа **Windows Mobile** при помощи Windows Media Player, и медиа-файлов с указанным содержимым, записываемых на устройства типа **Palm** или **iPhone-устройства**.
Специальные разрешения: Запись бэкапа	Определяет, создается ли теневая копия резервной копии данных с указанным содержимым, записываемой с ПК на iPhone-устройство.

Право теневого копирования	Описание
Специальные разрешения: Запись заметки	Определяет, создается ли теневая копия заметок с указанным содержимым, записываемых на мобильное устройство. Применимо к типам **iPhone-устройства**, **Palm** и **Windows Mobile**.
Специальные разрешения: Запись БД Pocket Access	Определяет, создается ли теневая копия баз данных Pocket Access с указанным содержимым, записываемых на устройство типа **Windows Mobile**.
Специальные разрешения: Запись задачи	Определяет, создается ли теневая копия задач с указанным содержимым, записываемых на мобильное устройство. Применимо к типам **Palm** и **Windows Mobile**.
Специальные разрешения: Запись расхода	Определяет, создается ли теневая копия данных приложения Palm Expense с указанным содержимым, записываемых на устройство типа **Palm**.
Специальные разрешения: Запись документа	Определяет, создается ли теневая копия документов с указанным содержимым, записываемых на устройство типа **Palm**.
Специальные разрешения: Запись неидентифицированного содержимого	Определяет, создается ли теневая копия прочих данных с указанным содержимым, записываемых на устройство типа **Windows Mobile**.
Специальные разрешения: Копирование текста	Определяет, создается ли теневая копия текстовых данных с указанным содержимым, вставляемых из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование файла	Определяет, создается ли теневая копия файлов с указанным содержимым, вставляемых из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование изображения	Определяет, создается ли теневая копия изображений с указанным содержимым, вставляемых из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование экрана	Определяет, создается ли теневая копия снимков экрана с указанным содержимым, вставляемых из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование неидентифицированного содержимого	Определяет, создается ли теневая копия прочих данных с указанным содержимым, вставляемых из буфера обмена. Применимо только к типу **Буфер обмена**.

Примечание: Права теневого копирования **Основные**, установленные для типа **Съемные устройства**, применяются только к незашифрованным устройствам. Права теневого копирования **Зашифрованные**, установленные для типа **Съемные устройства**, применяются только к зашифрованным устройствам. Чтобы установить права теневого копирования одновременно для зашифрованных и незашифрованных съемных устройств, необходимо одновременно задать права теневого копирования **Основные** и **Зашифрованные**.

Обнаружение контента

Контентно-зависимые правила, применяемые для операций обнаружения содержимого, позволяют распознавать попытки чтения, записи и удаления указанного содержимого с целью аудита и/или оповещения, не прибегая к блокированию доступа к контенту и его теневому копированию. Операции удаления и записи контролируются совместно при помощи права на запись.

Следующая таблица содержит сведения о правах, которые используются при создании контентно-зависимых правил данного типа.

Право обнаружения	Описание
Основные: Чтение	Определяет, выполняется ли обнаружение попыток чтения данных с указанным содержимым с устройства. Применимо только к типам **Оптический привод**, **Гибкий диск** и **Съемные устройства**.
Основные: Запись	Определяет, выполняется ли обнаружение попыток записи данных с указанным содержимым на устройство. Применимо только к типам **Гибкий диск** и **Съемные устройства**.
Основные: Чтение, Запись	Определяет, выполняется ли обнаружение попыток чтения или записи данных с указанным содержимым с/на устройство. Применимо к типам **Гибкий диск** и **Съемные устройства**.
Основные: Копирование в буфер обмена	Определяет, выполняется ли обнаружение попыток вставить данные с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Основные: Печать	Определяет, выполняется ли обнаружение попыток печати документов с указанным содержимым. Применимо только к типу **Принтер**.
Основные: Чтение с подключенного диска	Определяет, выполняется ли обнаружение попыток чтения данных с указанным содержимым с подключенного диска. Применимо только к типу **ТС-устройства**.
Основные: Запись на подключенный диск	Определяет, выполняется ли обнаружение попыток записи данных с указанным содержимым на подключенный диск. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена входящий текст	Определяет, выполняется ли обнаружение попыток вставить текстовые данные с указанным содержимым из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена входящие файлы	Определяет, выполняется ли обнаружение попыток вставить файлы с указанным содержимым из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена входящие изображения	Определяет, выполняется ли обнаружение попыток вставить изображения с указанным содержимым из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена входящие неизвестные данные	Определяет, выполняется ли обнаружение попыток вставить прочие данные с указанным содержимым из буфера обмена в окно терминальной сессии/виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена исходящий текст	Определяет, выполняется ли обнаружение попыток вставить текстовые данные с указанным содержимым из буфера обмена окна терминальной сессии /виртуальной машины. Применимо только к типу **ТС-устройства**.

Право обнаружения	Описание
Основные: Буфер обмена исходящие файлы	Определяет, выполняется ли обнаружение попыток вставить файлы с указанным содержимым из буфера обмена окна терминальной сессии /виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена исходящие изображения	Определяет, выполняется ли обнаружение попыток вставить изображения с указанным содержимым из буфера обмена окна терминальной сессии /виртуальной машины. Применимо только к типу **ТС-устройства**.
Основные: Буфер обмена исходящие неизвестные данные	Определяет, выполняется ли обнаружение попыток вставить прочие данные с указанным содержимым из буфера обмена окна терминальной сессии /виртуальной машины. Применимо только к типу **ТС-устройства**.
Зашифрованные: Чтение	Определяет, выполняется ли обнаружение попыток чтения данных с указанным содержимым с зашифрованного устройства. Применимо только к типу **Съемные устройства**.
Зашифрованные: Запись	Определяет, выполняется ли обнаружение попыток записи данных с указанным содержимым на зашифрованное устройство. Применимо только к типу **Съемные устройства**.
Зашифрованные: Чтение, Запись	Определяет, выполняется ли обнаружение попыток чтения или записи данных с указанным содержимым с/на зашифрованное устройство. Применимо только к типу **Съемные устройства**.
Специальные разрешения: Копирование текста	Определяет, выполняется ли обнаружение попыток вставить текстовые данные с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование файла	Определяет, выполняется ли обнаружение попыток вставить файлы с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование изображения	Определяет, выполняется ли обнаружение попыток вставить изображения с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование экрана	Определяет, выполняется ли обнаружение попыток вставить снимков экрана с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.
Специальные разрешения: Копирование неидентифицированного содержимого	Определяет, выполняется ли обнаружение попыток вставить прочие данные с указанным содержимым из буфера обмена. Применимо только к типу **Буфер обмена**.

Правила для протоколов

Контентно-зависимые правила расширяют базовую функциональность контроля доступа к сетевым протоколам в DeviceLock DLP, обеспечивая высокотехнологичный уровень защиты конфиденциальных документов организации посредством использования технологий контентного анализа и фильтрации содержимого файлов и данных. Они обеспечивают автоматическую проверку содержимого данных/файлов, передаваемых по сети, обнаружение конфиденциальных данных и применение необходимых политик безопасности.

С помощью контентно-зависимых правил можно выборочно разрешить или запретить доступ к указанному содержимому данных, передаваемых по сети, вне зависимости от разрешений, установленных на протокол. Контентно-зависимые правила можно также использовать, чтобы разрешить или запретить теневое копирование указанного содержимого, или для обнаружения попыток приема и передачи данных с определенным содержимым без блокирования доступа и без создания теневых копий. Правила можно задавать применительно к тем или иным протоколам индивидуально для различных пользователей и/или групп.

Контентно-зависимые правила могут быть заданы для операций контроля доступа, теневого копирования, обнаружения содержимого, или для любой комбинации этих операций.

Следующие примеры демонстрируют использование контентно-зависимых правил.

- **Пример 1 - Использование контентно-зависимых правил для операций контроля доступа**. Можно запретить отдельным пользователям или группам отправку файлов, содержащих номера кредитных карт, номера телефонов и почтовые адреса, на FTP-сервер.
- **Пример 2 - Использование контентно-зависимых правил для операций теневого копирования**. Для проведения аудита информационной безопасности и в целях расследования инцидентов информационной безопасности можно указать, что теневые копии будут созданы для мгновенных сообщений, содержащих номера кредитных карт и адреса электронной почты.
- **Пример 3 - Использование контентно-зависимых правил для операций обнаружения.** Можно задать правило, предусматривающее протоколирование и отправку тревожного оповещения при попытках передачи исполняемых файлов, без блокирования передачи или создания теневых копий таких файлов.

Узел “Контентно-зависимые правила”

Под узлом **Протоколы** > **Контентно-зависимые правила** в дереве консоли перечисляются пользователи и группы, для которых заданы контентно-зависимые правила, относящиеся к протоколам. Контентно-зависимые правила могут быть заданы индивидуально для каждого пользователя и группы.

Примечание: Можно задавать различные контентно-зависимые правила для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Контентно-зависимые правила для оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Контентно-зависимые правила для автономного режима (офлайн-профиль) применяются, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Описание политик DeviceLock для автономного режима можно найти в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по настройке контентно-зависимых правил см. в разделе Управление контентно-зависимыми правилами для автономного режима.

Контекстное меню узла **Контентно-зависимые правила** содержит следующие команды:

- **Управление** - Открывает диалоговое окно, позволяющее задать или отредактировать контентно-зависимые правила для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее задать или отредактировать контентно-зависимые правила для автономного режима.
- **Загрузить** - Позволяет импортировать ранее сохраненный файл с контентно-зависимыми правилами для оперативного режима.
- **Загрузить офлайновые настройки** - Позволяет импортировать ранее сохраненный файл с контентно-зависимыми правилами для автономного режима.
- **Сохранить** - Позволяет экспортировать контентно-зависимые правила, заданные для оперативного режима, в файл с расширением .cwl, который затем можно импортировать и использовать на другом компьютере.
- **Сохранить офлайновые настройки** - Позволяет экспортировать контентно-зависимые правила, заданные для автономного режима, в файл с расширением .cwl, который затем можно импортировать и использовать на другом компьютере.
- **Сбросить** - Сбрасывает контентно-зависимые правила для оперативного режима в состояние “не задано”. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.
- **Сбросить офлайновые настройки** - Сбрасывает контентно-зависимые правила для автономного режима в состояние “не задано”. Если такие правила не заданы, к клиентским компьютерам, находящимся не в сети, применяются правила, заданные для оперативного режима.
- **Удалить офлайновые настройки** - Блокирует наследование контентно-зависимых правил, заданных для автономного режима, и принудительно применяет правила, заданные для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

Пользователи и группы, для которых заданы контентно-зависимые правила, отображаются под узлом **Контентно-зависимые правила** в дереве консоли и имеют такое же контекстное меню, что и этот узел, за исключением команды **Сбросить офлайновые настройки** и с добавлением команды **Удалить пользователя**, которая удаляет контентно-зависимые правила для выбранного пользователя или группы.

Подробнее см. в разделах:

Настройка контентных групп

Управление контентно-зависимыми правилами

Список контентно-зависимых правил для протоколов

Пользователи и группы, для которых заданы контентно-зависимые правила, относящиеся к протоколам, отображаются под узлом **Протоколы** > **Контентно-зависимые правила** в дереве консоли (подробнее см. в разделе Узел "Контентно-зависимые правила").

Если выбрать пользователя или группу под узлом **Контентно-зависимые правила** в дереве консоли, на панели сведений отображаются контентно-зависимые правила, заданные для этого пользователя или группы. Для каждого правила список содержит следующие сведения:

- **Имя** - Имя правила. По умолчанию контентно-зависимое правило имеет то же имя, что и указанная в правиле контентная группа.
- **Тип** - Тип анализа содержимого файла. Возможные значения:
  - **Определение типа файла** - Означает, что идентификация файлов ведется по сигнатурам.
  - **Ключевые слова** - Означает, что идентификация данных/файлов ведется по заданным ключевым словам и выражениям.
  - **Шаблон -** Означает, что идентификация данных/файлов ведется на основе заданных шаблонов регулярных выражений Perl.
  - **Свойства документа -** Означает, что идентификация файлов ведется по их свойствам.
  - **Цифровые отпечатки** - Означает, что идентификация данных/файлов ведется по их цифровым отпечаткам.
  - **Составное -** Означает, что идентификация данных/файлов ведется по заданному контенту, описанному логическим выражением.
- **Действие** - Показывает, какие действия с протоколами пользователю разрешены или запрещены, а также какие действия пользователя будут записываться в журнале теневого копирования.
- **Применяется к** - Возможные значения:
  - **Разрешения** - Означает, что правило применяется для операций контроля доступа.
  - **Теневое копирование** - Означает, что правило применяется к операциям избирательного теневого копирования.
  - **Обнаружение** - Означает, что правило применяется к операциям обнаружения.
  - **Разрешения+Теневое копирование** - Означает, что правило применяется к операциям контроля доступа и операциям избирательного теневого копирования.
  - **Разрешения+Обнаружение** - Означает, что правило применяется к операциям контроля доступа и операциям обнаружения.
  - **Теневое копирование+Обнаружение** - Означает, что правило применяется к операциям избирательного теневого копирования и операциям обнаружения.
  - **Разрешения+Теневое копирование+Обнаружение** - Означает, что правило применяется ко всем возможным видам операций: контроля доступа, избирательного теневого копирования и обнаружения содержимого.
- **Протокол(ы)** - Протоколы, к которым применяется правило.

- **Отправить алерт** - Отображает, включены ли оповещения для данного правила.
- **Протоколировать событие** - Отображает, включена ли регистрация событий в журнале аудита для данного правила.
- **Теневое копирование** - Отображает, будет ли создана теневая копия в результате срабатывания данного правила.
- **Профиль** - Возможные значения: **Обычный** и **Офлайн**. Значение **Обычный** указывает, что правило применяется к компьютерам, находящимся в сети. Значение **Офлайн** указывает, что правило применяется к компьютерам, работающим автономно.

  Одним и тем же пользователям или группам можно задавать разные правила для разных профилей. О работе с правилами офлайн-профиля см. в разделе Управление контентно-зависимыми правилами для протоколов в автономном режиме.

Контекстное меню правила в списке на панели сведений содержит следующие команды:

- **Управление** - В зависимости от профиля данного правила (обычный или офлайн), открывает диалоговое окно, в котором можно задать контентно-зависимые правила для оперативного или автономного режима.
- **Редактировать** - Открывает диалоговое окно, в котором можно просмотреть или изменить данное правило.
- **Отправить алерт** - Включает или отключает отправку оповещений для данного правила.
- **Протоколировать событие** - Включает или отключает протоколирование событий для данного правила.
- **Теневое копирование** - Включает или отключает теневое копирование контента, вызывающего срабатывание данного правила.
- **Удалить** - Удаляет данное правило.

Подробнее см. в разделе Управление контентно-зависимыми правилами.

Управление доступом к контенту

Контентно-зависимые правила для протоколов позволяют:

- Предоставить доступ к указанному контенту, когда доступ запрещен на уровне протокола.
- Запретить доступ к указанному контенту, когда доступ разрешен на уровне типа протокола.

Контентно-зависимые правила применяются к сессиям, разрешенным по белому списку протоколов, только если установлен флажок Контентный анализ. В противном случае контентно-зависимые правила не влияют на такие сессии.

Следующая таблица содержит сведения о правах доступа, которые используются при создании контентно-зависимых правил для протоколов.

Протокол	Права доступа	Описание
Поиск работы	Основные: Поиск	Право отправлять запросы поиска вакансий с указанным содержимым на сайты поиска работы.
	Основные: Исходящие сообщения	Право отправлять сообщения, резюме и другие данные с указанным содержимым через веб-формы на сайтах поиска работы.
	Основные: Исходящие файлы	Право загружать файлы с указанным содержимым на сайты поиска работы.
Файловые хранилища, HTTP	Основные: POST-запросы	Право отправлять данные веб-форм с указанным содержимым на веб-сервер, используя HTTP.
	Основные: Исходящие файлы	Право отправлять файлы с указанным содержимым на веб-сервер, используя HTTP.
	SSL: POST-запросы	Право отправлять данные веб-форм с указанным содержимым на веб-сервер, используя HTTPS.
	SSL: Исходящие файлы	Право отправлять файлы с указанным содержимым на веб-сервер, используя HTTPS.
FTP	Основные: Исходящие файлы	Право отправлять файлы с указанным содержимым на FTP-сервер.
	SSL: Исходящие файлы	Право отправлять файлы с указанным содержимым на FTP-сервер, используя FTPS.
IBM Notes	Основные: Исходящие сообщения	Право отправлять почтовые сообщения с указанным содержимым из почтового клиента IBM Notes на сервер IBM Domino.
	Основные: Исходящие файлы	Право отправлять вложения с указанным содержимым из почтового клиента IBM Notes на сервер IBM Domino.

Протокол	Права доступа	Описание
ICQ Messenger, IRC	Основные: Исходящие сообщения	Право отправлять мгновенные сообщения с указанным содержимым.
	Основные: Исходящие файлы	Право отправлять файлы с указанным содержимым.
	SSL: Исходящие сообщения	Право отправлять мгновенные сообщения с указанным содержимым, используя SSL.
	SSL: Исходящие файлы	Право отправлять файлы с указанным содержимым, используя SSL.
Mail.ru Агент, Jabber, Skype, Zoom	Основные: Исходящие сообщения	Право отправлять мгновенные сообщения с указанным содержимым.
	Основные: Исходящие файлы	Право отправлять файлы с указанным содержимым.
MAPI	Основные: Исходящие сообщения	Право отправлять почтовые сообщения с указанным содержимым из клиентского приложения Outlook на Microsoft Exchange Server.
	Основные: Исходящие файлы	Право отправлять вложения с указанным содержимым из клиентского приложения Outlook на Microsoft Exchange Server.
SMB	Основные: Исходящие файлы	Право загружать файлы с указанным содержимым на SMB-серверы, а также скачивать такие файлы из общих сетевых папок компьютера, на котором работает сервис DeviceLock.
SMTP, Web-почта	Основные: Исходящие сообщения	Право отправлять сообщения электронной почты с указанным содержимым.
	Основные: Исходящие файлы	Право отправлять вложения электронной почты с указанным содержимым.
	SSL: Исходящие сообщения	Право отправлять сообщения электронной почты с указанным содержимым, используя SSL.
	SSL: Исходящие файлы	Право отправлять вложения электронной почты с указанным содержимым, используя SSL.
Социальные сети	Основные: Исходящие сообщения	Право отправлять сообщения и комментарии с указанным содержимым.
	Основные: Исходящие файлы	Право отправлять медиа-файлы и другие файлы с указанным содержимым на сайт социальной сети.
Viber	Основные: Исходящие файлы	Право отправлять файлы с указанным содержимым.
Web-поиск	Основные: Поиск	Право отправлять поисковые запросы с указанным содержимым на сайты веб-поиска.

Примечание:

- Если для какого-либо протокола установлено разрешение “Нет доступа” (доступ запрещен), и при этом задано контентно-зависимое правило, разрешающее доступ к указанному содержимому для этого протокола, пользователь автоматически получает право **Отправка/Получение данных**. Подробнее об этом праве см. в разделе Разрешения на доступ к протоколам.
- Если для протокола **Viber** установлено разрешение “Нет доступа”, то контентно-зависимые правила, разрешающие доступ к указанному содержимому для этого протокола, не действуют. В этом случае пользователь Viber не может ни отправлять, ни получать сообщения и файлы.
- Право **POST-запросы** для протокола **Файловые хранилища**, будучи примененным к сервису iCloud, определяет право пользователя на загрузку не-файловых данных (почта, заметки, календарь, контакты, напоминания) в облако iCloud. Аналогичное право определяет совершение аудита и теневого копирования не-файловых данных, загружаемых на iCloud. В записях аудита и теневых копиях этих данные идентифицируются как **Исходящие сообщения**.
- Права доступа для протокола **MAPI** также применяются к черновикам сообщений, не отправленных из Outlook на Exchange Server. Например, DeviceLock не позволит Outlook автоматически сохранять черновики сообщений с указанным контентом, если пользователь Outlook не имеет права отправлять сообщения с этим контентом.

При использовании контентно-зависимых правил необходимо учитывать следующее:

- Запрещающие контентно-зависимые правила имеют приоритет над разрешающими правилами, если правила применяются для одного и того же пользователя или группы пользователей.

  Исключение: Разрешающее контентно-зависимое правило на основе группы свойств документа с выбранной опцией **Извлечение текста не поддерживается** имеет приоритет над запрещающими правилами, позволяя передавать любой подходящий под это правило контент, в том числе части многотомных архивов.

  Исключение: Разрешающее контентно-зависимое правило на основе группы свойств документа с выбранной опцией **Защищено паролем** имеет приоритет над запрещающими правилами, позволяя передавать любой подходящий под это правило контент. Разрешающее комплексное правило будет иметь приоритет только в том случае, если в числе групп разрешающей логической цепочки, с которыми совпал файл, будет группа свойств документа с выбранной опцией **Защищено паролем**.

  Исключение: Разрешающее контентно-зависимое правило на основе группы цифровых отпечатков с выбранной опцией **Точное совпадение файла** имеет приоритет над запрещающими правилами, позволяя передавать любой подходящий под это правило контент. Разрешающее комплексное правило будет иметь приоритет только в том случае, если в числе групп разрешающей логической цепочки, с которыми совпал файл, будет группа цифровых отпечатков с выбранной опцией **Точное совпадение файла**.

- Разрешающие контентно-зависимые правила разрешают передачу целиком всего объекта данных (сообщения или файла, включая архивы и контейнеры), если в нем присутствует содержимое, удовлетворяющее этим правилам и отсутствует содержимое, явно запрещенное запрещающими контентно-зависимыми правилами.
- Проверка содержимого файлов может отнимать много времени. Можно указать сообщение о проверке содержимого, которое будет отображаться пользователям во время проверки. Подробнее об этом сообщении см. в описании параметра Сообщение о проверке содержимого.
- Когда контентно-зависимые правила запрещают передачу некоторого контента, пользователя уведомляют об этом определенным сообщением при условии, что в настройках сервиса DeviceLock включен параметр Контентно-зависимое сообщение о блокировании записи.

Теневое копирование контента

Прежде чем можно будет использовать контентно-зависимые правила для операций теневого копирования, необходимо включить теневое копирование в разделе **Аудит, Теневое копирование и Алерты** на уровне протокола. Контентно-зависимые правила, применяемые к операциям теневого копирования, позволяют фильтровать теневые копии данных и файлов, передаваемых пользователями.

Следующая таблица содержит сведения о правах теневого копирования, которые используются при создании контентно-зависимых правил для протоколов.

Протокол	Права теневого копирования	Описание
Поиск работы	Основные: Поиск	Определяет, создается ли теневая копия запросов поиска вакансий с указанным содержимым при их отправке на сайты поиска работы.
	Основные: Исходящие сообщения	Определяет, создается ли теневая копия сообщений, резюме и других данных с указанным содержимым при их отправке через веб-формы на сайтах поиска работы.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их загрузке на сайты поиска работы.
HTTP, Файловые хранилища	Основные: Входящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их скачивании с веб-сервера.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их загрузке на веб-сервер.
	Основные: POST-запросы	Определяет, создается ли теневая копия данных веб-форм с указанным содержимым при их отправке на веб-сервер.
	SSL: Входящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их скачивании с веб-сервера с использованием HTTPS.
	SSL: Исходящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их загрузке на веб-сервер с использованием HTTPS.
	SSL: POST-запросы	Определяет, создается ли теневая копия данных веб-форм с указанным содержимым при их правке на веб-сервер с использованием HTTPS.

Примечание: Право POST-запросы для протокола Файловые хранилища, примененное к сервису iCloud, разрешает теневое копирование не-файловых данных (почта, заметки, календарь, контакты, напоминания).

Протокол	Права теневого копирования	Описание
FTP	Основные: Входящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их скачивании с FTP-сервера.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их загрузке на FTP-сервер.
	SSL: Входящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их скачивании с FTP-сервера с использованием FTPS.
	SSL: Исходящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым при их загрузке на FTP-сервер с использованием FTPS.
IBM Notes	Основные: Входящие сообщения	Определяет, создается ли теневая копия почтовых сообщений с указанным содержимым, получаемых клиентом IBM Notes от сервера IBM Domino.
	Основные: Входящие файлы	Определяет, создается ли теневая копия почтовых вложений с указанным содержимым, получаемым клиентом IBM Notes от сервера IBM Domino.
	Основные: Исходящие сообщения	Определяет, создается ли теневая копия почтовых сообщений с указанным содержимым, отправляемых клиентом IBM Notes на сервер IBM Domino.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия почтовых вложений с указанным содержимым, отправляемых клиентом IBM Notes на сервер IBM Domino.

Протокол	Права теневого копирования	Описание
ICQ Messenger, IRC	Основные: Входящие сообщения	Определяет, создается ли теневая копия входящих мгновенных сообщений с указанным содержимым.
	Основные: Входящие файлы	Определяет, создается ли теневая копия входящих файлов с указанным содержимым.
	Основные: Исходящие сообщения	Определяет, создается ли теневая копия исходящих мгновенных сообщений с указанным содержимым.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия исходящих файлов с указанным содержимым.
	SSL: Входящие сообщения	Определяет, создается ли теневая копия входящих мгновенных сообщений с указанным содержимым, полученных по SSL.
	SSL: Входящие файлы	Определяет, создается ли теневая копия входящих файлов с указанным содержимым, полученных по SSL.
	SSL: Исходящие сообщения	Определяет, создается ли теневая копия исходящих мгновенных сообщений с указанным содержимым, отправленных по SSL.
	SSL: Исходящие файлы	Определяет, создается ли теневая копия исходящих файлов с указанным содержимым, отправленных по SSL.
Jabber, Mail.ru Агент, Skype, Telegram, Viber, WhatsApp, Zoom	Основные: Входящие сообщения	Определяет, создается ли теневая копия входящих мгновенных сообщений с указанным содержимым.
	Основные: Входящие файлы	Определяет, создается ли теневая копия входящих файлов с указанным содержимым.
	Основные: Исходящие сообщения	Определяет, создается ли теневая копия исходящих мгновенных сообщений с указанным содержимым.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия исходящих файлов с указанным содержимым.
MAPI	Основные: Входящие сообщения	Определяет, создается ли теневая копия почтовых сообщений с указанным содержимым, полученных клиентом Outlook от сервера Microsoft Exchange.
	Основные: Входящие файлы	Определяет, создается ли теневая копия почтовых вложений с указанным содержимым, полученных клиентом Outlook от сервера Microsoft Exchange.
	Основные: Исходящие сообщения	Определяет, создается ли теневая копия почтовых сообщений с указанным содержимым, отправленных клиентом Outlook на сервер Microsoft Exchange.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия почтовых вложений с указанным содержимым, отправленных клиентом Outlook на сервер Microsoft Exchange.

Протокол	Права теневого копирования	Описание
SMB	Основные: Входящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым, которые пользователь скачивает с SMB-сервера или загружает в общие сетевые папки компьютера, на котором работает сервис DeviceLock.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия файлов с указанным содержимым, которые пользователь загружает на SMB-сервер или скачивает из общих сетевых папок компьютера, на котором работает сервис DeviceLock.
SMTP, Web-почта	Основные: Исходящие сообщения	Определяет, создается ли теневая копия исходящих сообщений электронной почты с указанным содержимым.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия исходящих вложений электронной почты с заданным содержимым.
	SSL: Исходящие сообщения	Определяет, создается ли теневая копия исходящих сообщений электронной почты с указанным содержимым, отправляемых по SSL.
	SSL: Исходящие файлы	Определяет, создается ли теневая копия исходящих вложений электронной почты с указанным содержимым, отправляемых по SSL.
Социальные сети	Основные: Исходящие сообщения	Определяет, создается ли теневая копия исходящих сообщений и комментариев с указанным содержимым.
	Основные: Исходящие файлы	Определяет, создается ли теневая копия исходящих медиа-файлов и других файлов с указанным содержимым.
Web-поиск	Основные: Поиск	Определяет, создается ли теневая копия запросов веб-поиска с указанным содержимым.

Обнаружение контента

Следующая таблица содержит сводную информацию о правах, которые могут быть заданы в контентно-зависимых правилах для операций обнаружения содержимого.

Протокол	Права доступа	Описание
Поиск работы	Основные: Поиск	Определяет, выполняется ли обнаружение попыток поиска вакансий с указанным содержимым на сайтах поиска работы.
	Основные: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправки сообщений, резюме и других данных с указанным содержимым через веб-формы на сайтах поиска работы.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток загрузить файлы с указанным содержимым на сайты поиска работы.
Файловые хранилища, HTTP	Основные: Входящие файлы	Определяет, выполняется ли обнаружение попыток скачать файлы с указанным содержимым с веб-сервера.
	Основные: POST-запросы	Определяет, выполняется ли обнаружение попыток отправить данные веб-форм с указанным содержимым на веб-сервер.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток загрузить файлы с указанным содержимым на веб-сервер.
	SSL: Входящие файлы	Определяет, выполняется ли обнаружение попыток скачать файлы с указанным содержимым с веб-сервера с использованием HTTPS.
	SSL: POST-запросы	Определяет, выполняется ли обнаружение попыток отправить данные веб-форм с указанным содержимым на веб-сервер с использованием HTTPS.
	SSL: Исходящие файлы	Определяет, выполняется ли обнаружение попыток загрузить файлы с указанным содержимым на веб-сервер с использованием HTTPS.
FTP	Основные: Входящие файлы	Определяет, выполняется ли обнаружение попыток скачать файлы с указанным содержимым с FTP сервера.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток загрузить файлы с указанным содержимым на FTP сервер.
	SSL: Входящие файлы	Определяет, выполняется ли обнаружение попыток скачать файлы с указанным содержимым с FTP сервера с использованием FTPS.
	SSL: Исходящие файлы	Определяет, выполняется ли обнаружение попыток загрузить файлы с указанным содержимым на FTP сервер с использованием FTPS.

Протокол	Права доступа	Описание
IBM Notes	Основные: Входящие сообщения	Определяет, выполняется ли обнаружение попыток получить почтовые сообщения с указанным содержимым с сервера IBM Domino на клиент IBM Notes.
	Основные: Входящие файлы	Определяет, выполняется ли обнаружение попыток получить почтовые вложения с указанным содержимым с сервера IBM Domino на клиент IBM Notes.
	Основные: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправить почтовые сообщения с указанным содержимым с клиента IBM Notes на сервер IBM Domino.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток отправить почтовые вложения с указанным содержимым с клиента IBM Notes на сервер IBM Domino.
ICQ Messenger, IRC	Основные: Входящие сообщения	Определяет, выполняется ли обнаружение попыток получить мгновенные сообщения с указанным содержимым.
	Основные: Входящие файлы	Определяет, выполняется ли обнаружение попыток получить файлы с указанным содержимым.
	Основные: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправить мгновенные сообщения с указанным содержимым.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток отправить файлы с указанным содержимым.
	SSL: Входящие сообщения	Определяет, выполняется ли обнаружение попыток получить мгновенные сообщения с указанным содержимым по SSL.
	SSL: Входящие файлы	Определяет, выполняется ли обнаружение попыток получить файлы с указанным содержимым по SSL.
	SSL: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправить мгновенные сообщения с указанным содержимым по SSL.
	SSL: Исходящие файлы	Определяет, выполняется ли обнаружение попыток отправить файлы с указанным содержимым по SSL.

Протокол	Права доступа	Описание
Jabber, Mail.ru Агент, Skype, Telegram, Viber, WhatsApp, Zoom	Основные: Входящие сообщения	Определяет, выполняется ли обнаружение попыток получить мгновенные сообщения с указанным содержимым.
	Основные: Входящие файлы	Определяет, выполняется ли обнаружение попыток получить файлы с указанным содержимым.
	Основные: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправить мгновенные сообщения с указанным содержимым.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток отправить файлы с указанным содержимым.
MAPI	Основные: Входящие сообщения	Определяет, выполняется ли обнаружение попыток получить почтовые сообщения с указанным содержимым с сервера Microsoft Exchange в приложение Outlook.
	Основные: Входящие файлы	Определяет, выполняется ли обнаружение попыток получить почтовые вложения с указанным содержимым с сервера Microsoft Exchange в приложение Outlook.
	Основные: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправить почтовые сообщения с указанным содержимым из приложения Outlook на сервер Microsoft Exchange.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток отправить почтовые вложения с указанным содержимым из приложения Outlook на сервер Microsoft Exchange.

Примечание: Права доступа для протокола MAPI, относящиеся к операциям обнаружения, также применяются к черновикам сообщений, не отправленных из Outlook на Exchange Server. Так, если пользователь Outlook имеет право отправлять сообщения с указанным контентом, DeviceLock обнаруживает сохраненные черновики таких сообщений, когда пользователь закрывает Outlook без их отправки. Если у пользователя нет права на отправку таких сообщения, сообщение с указанным контентом будет обнаруживаться при сохранении его черновика в Outlook.

Протокол	Права доступа	Описание
SMB	Основные: Входящие файлы	Определяет, выполняется ли обнаружение попыток скачать файлы с указанным содержимым с SMB-сервера или загрузить такие файлы в общие сетевые папки компьютера, на котором работает сервис DeviceLock.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток загрузить файлы с указанным содержимым на SMB-сервер или скачать такие файлы из общих сетевых папок компьютера, на котором работает сервис DeviceLock.
SMTP, Web-почта	Основные: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправить сообщения электронной почты с указанным содержимым.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток отправить вложения электронной почты с указанным содержимым.
	SSL: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправить сообщения электронной почты с указанным содержимым по SSL.
	SSL: Исходящие файлы	Определяет, выполняется ли обнаружение попыток отправить вложения электронной почты с указанным содержимым по SSL.
Социальные сети	Основные: Исходящие сообщения	Определяет, выполняется ли обнаружение попыток отправить сообщения или комментарии с указанным содержимым.
	Основные: Исходящие файлы	Определяет, выполняется ли обнаружение попыток отправить медиа-файлы или другие файлы с указанным содержимым.
Web-поиск	Основные: Поиск	Определяет, выполняется ли обнаружение попыток отправить поисковые запросы с указанным содержимым на сайты веб-поиска.

Настройка контентных групп

Контентно-зависимые правила создаются на основе контентных групп, позволяющих централизованно задавать типы контента, которые требуют контроля. Контентные группы определяют критерии контентной фильтрации для выявления данных, к которым должны применяться правила.

Все контентные группы хранятся в базе данных контента. Для устройств и протоколов используется одна и та же база данных контента. Эта база данных является частью политики сервиса DeviceLock и, соответственно, сохраняется в файлах с настройками сервиса, созданных при помощи консоли DeviceLock Management Console, DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

В следующих разделах описываются имеющиеся типы контентных групп, а также предоставляются инструкции по созданию пользовательских групп для каждого типа:

- Группы определения типа файла - Выявление файлов по сигнатурам файловых типов.
- Группы ключевых слов - Поиск указанных ключевых слов или фраз в файлах/данных.
- Группы шаблонов - Поиск фрагментов текста при помощи регулярных выражений Perl.
- Группы свойств документа - Поиск документов с определенными свойствами (например, имя документа, его размер, заголовок, тема и т.п.).
- Группы цифровых отпечатков - Проверка цифровых отпечатков файлов или данных.
- Составные группы - Построение логического выражения из групп различных типов.

Настройка контентных групп предполагает также:

- Просмотр встроенных контентных групп
- Дублирование встроенных контентных групп
- Редактирование или удаление пользовательских контентных групп
- Тестирование контентных групп

Группы определения типа файла

Группы определения типа файла используются для контроля доступа к файлам на основании их типа, определяемого по цифровой сигнатуре файла. Эти группы содержат определения типов файлов, для каждого из которых отображается расширение файла (например, DOC) и описание (например, документ Microsoft Word). Правило, созданное на основе группы определения типа файла, применяется ко всем типам файлов, включенным в эту группу.

Поисковый сервер предоставляет широкий выбор предопределенных (встроенных) групп этого типа. Можно использовать встроенные в их исходном виде, создавать их редактируемые копии (дубликаты) или создавать новые группы для решения частных задач организации.

Встроенные группы облегчают задачу настройки контентно-зависимых правил, позволяя во многих случаях обойтись без создания пользовательских групп.

Примечание: Имеется возможность просмотра параметров любой встроенной группы, однако изменять параметры встроенных групп или удалять такие группы невозможно. Подробнее см. в разделе Просмотр встроенных контентных групп.

В следующей таблице перечислены все встроенные группы данного типа:

Встроенные контентные группы определения типа файла

Android	MS Word
BlackBerry	MS Works
Common Object File Format (COFF)	OpenOffice, StarOffice, OpenDocument и т.д.
FileMaker Pro	PDF, PostScript и XPS-документы
iOS	QuickBooks, Quicken, TurboTax и т.д.
Lotus SmartSuite	Rich text-документы
MS Access	Text, HTML и XML
MS Excel	WordPerfect Office
MS InfoPath	Архивы
MS Money	Аудио, Видео, Flash
MS OneNote	Базы данных
MS Outlook, Outlook Express и почтовые архивы	Изображения, чертежи, CAD
MS PowerPoint	Исполняемые файлы
MS Project	Сертификаты безопасности
MS Publisher	Файлы виртуальных машин
MS Visio	Файлы справки
MS Windows Installer	Факсы
MS Windows дампы памяти	Шрифты

Примечание:

- Контентно-зависимые правила поддерживают следующие форматы документов, используемых на Palm-устройствах: Word To Go, Sheet To Go и Slideshow To Go. Формат Word To Go включен во встроенные группы MS Word и Rich Text Format, формат Sheet To Go включен во встроенную группу MS Excel, а формат Slideshow To Go включен во встроенную группу MS PowerPoint.
- Файлы Microsoft Word, Rich Text Format (RTF), Excel и PowerPoint могут переноситься на Palm-устройство с помощью приложения Documents To Go, которое конвертирует указанные файлы в специальный формат: файлы Word и RTF конвертируются в формат Word To Go, файлы Excel конвертируются в формат Sheet To Go, и файлы PowerPoint конвертируются в формат Slideshow To Go. После конвертации файлы автоматически переносятся на Palm в процессе синхронизации.

Создание пользовательских групп определения типа файла

Контентно-зависимые правила можно создавать на основе собственных (пользовательских) контентных групп, если предопределенные (встроенные) контентные группы не отвечают вашим нуждам. Пользовательские группы определения типа файла могут быть заданы как сочетание любых типов файлов внутри одной группы, чтобы наилучшим образом решить задачи организации.

Например, предположим, что требуется предоставить определенным пользователям доступ к документам Word, Excel, PDF, а также к графическим файлам. Для этого следует сначала создать новую группу определения типа файла, в которую будут входить указанные типы содержимого. Затем следует создать правило на основе этой пользовательской группы.

Чтобы создать пользовательскую группу определения типа файла

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

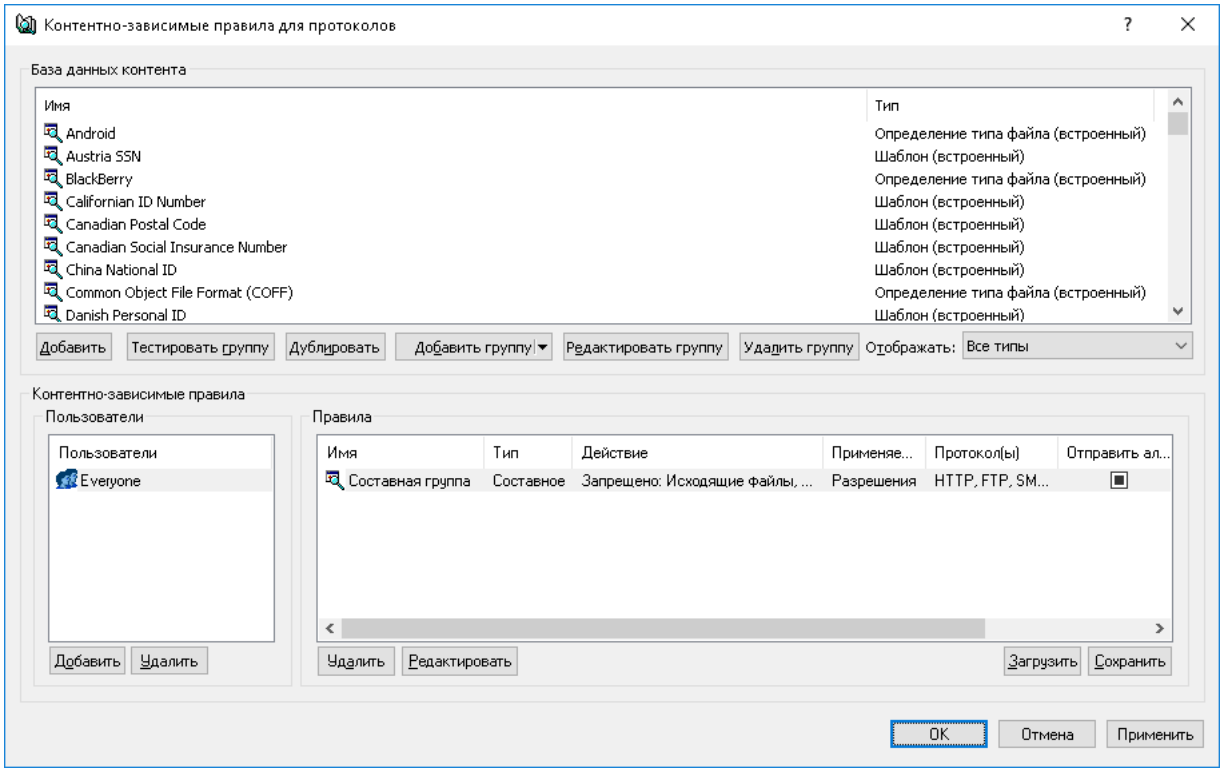
2. Раскройте узел **Устройства** либо узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

     - или -

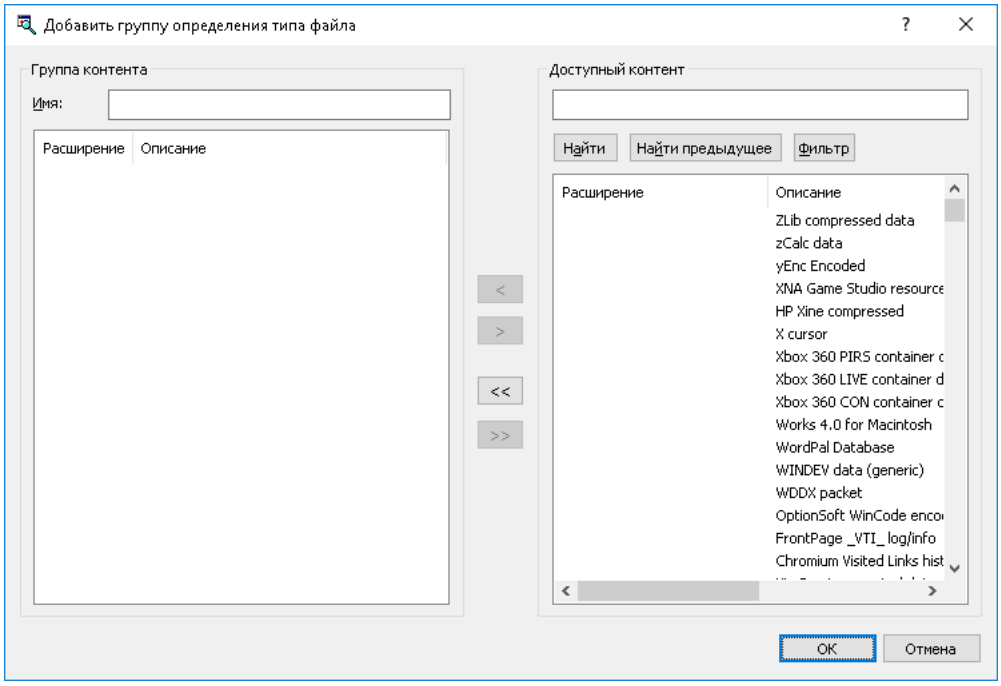
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

Появится диалоговое окно, подобное приведенному ниже.



4. В верхней части появившегося диалогового окна в области **База данных контента** нажмите стрелку рядом с полем **Добавить группу**, а затем выберите пункт **Определение типа файла**.

   Появится диалоговое окно "Добавить группу определения типа файла"



5. В левой части диалогового окна **Добавить группу определения типа файла** в области **Группа контента** введите имя новой контентной группы в поле **Имя**.
6. В правой части диалогового окна **Добавить группу определения типа файла** в области **Доступный контент** выберите любой тип файла, который требуется добавить в новую контентную группу, а затем нажмите кнопку <.

   Чтобы выбрать одновременно несколько типов файлов, используйте клавиши SHIFT или CTRL.

   Чтобы удалить отдельные типы файла из контентной группы, используйте кнопку >. Чтобы добавить или удалить все доступные типы файла в или из контентной группы одновременно, используйте кнопку << или >>.

   Примечание: Можно проводить поиск необходимых типов файлов по расширению или описанию в базе данных контента. Для поиска типов файла можно использовать знаки подстановки, такие как звездочка (*) и знак вопроса (?). Чтобы найти нужный тип файла или нужную группу типов файлов, в области **Доступный контент** введите расширение или описание файла со знаками подстановки или без них в строку поиска, а затем нажмите кнопку **Найти**. Чтобы применить фильтр к типам файлов, нажмите кнопку **Фильтр**. Чтобы удалить фильтр, примените фильтр к пустой строке поиска.

   Звездочка (*) заменяет любое количество символов. Знак вопроса (?) заменяет отдельный символ. Эти знаки подстановки можно использовать в любой части имени и в любом количестве.

7. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Добавить группу определения типа файла**.

   Новая контентная группа добавляется в список существующих контентных групп в области "База данных контента" в верхней части диалогового окна для управления контентно-зависимыми правилами.

Группы ключевых слов

Группы ключевых слов используются для контроля доступа к файлам, основанного на поиске заданных слов или фраз в документах.

DeviceLock предоставляет более 160 предопределенных (встроенных) групп ключевых слов, которые можно использовать для настройки прав доступа и/или операций теневого копирования. Можно использовать встроенные группы "как есть", создавать их редактируемые копии (дубликаты) или создавать собственные группы, необходимые для решения частных задач организации.

Встроенные группы облегчают задачу настройки контентно-зависимых правил, позволяя во многих случаях обойтись без создания пользовательских групп.

Примечание: Имеется возможность просмотра параметров любой встроенной группы, однако изменять параметры встроенных групп или удалять такие группы невозможно. Подробнее см. в разделе Просмотр встроенных контентных групп.

В следующей таблице перечислены все встроенные группы данного типа:

Встроенные контентные группы ключевых слов

FITS Date & Time	Корпоративный капитал (русск.)
FITS File Checksum	Кредитная история (англ.)
FITS File Descriptors	Кредиты (англ.)
FITS Hierarchical file grouping	Кредиты и займы (русск.)
FITS Instrumentorum	Мат (англ.)
FITS Non-standard	Мат (русск.)
FITS Observations	Медицина: действующие вещества (русск.)
FITS Standard	Медицина: лекарства (русск.)
Grades	Медицина: термины (русск.)
HCFA (CMS) 1500 Form	Медицинские диагнозы (англ.)
HIPAA - Diseases	Международная экономическая деятельность (русск.)
HIPAA HCPCS	Место рождения (амер.)
HIPAA ICD 10 - Diseases and Injuries	Названия бизнес-партнеров (англ.)
HIPAA ICD 10 - Drugs and Chemicals	Наркотики (англ.)
HIPAA ICD9	Нарушение закона (англ.)
HIPAA NDC Classes	Нарушение закона (русск.)
HIPAA NDC Dosages	Нарушение обязательств (англ.)
HIPAA NDC Listing	Нарушение обязательств (русск.)
HIPAA NDC Routes	Нарушение стандартов (англ.)
Japan: Surname in Hiragana	Насилие (англ.)
Japan: Surname in Kanji	Насилие (русск.)
Japan: Surname in Katakana	Национальные/этнические темы (англ.)
Japan: Surname in One-Byte Katakana	Недвижимость (англ.)
MEMO	Недовольство (англ.)

Встроенные контентные группы ключевых слов

PCI GLBA	Непристойные выражения (англ.)
Pro Earnings	Несоответствие нормам (русск.)
Sarbanes-Oxley Sensitive	Номер водительского удостоверения (амер.)
Security Agencies	Номера медицинских карт (амер.)
Sensitive Disease	Обучение персонала (англ.)
UB04 Form	Общие медицинские термины (англ.)
Азартные игры (англ.)	Оружие (англ.)
Американский адрес (англ.)	Отчет о подозрительной активности (англ.)
Американское имя (англ.)	Отчет о соответствии (англ.)
Банковские выписки (англ.)	Ошибки (англ.)
Банковские операции (русск.)	Ошибки (русск.)
Банковские операции: участники (русск.)	Пароли (англ.)
Банковские переводы (англ.)	Пароли и коды доступа (русск.)
Банковский ABA-номер (англ.)	Патенты и торговые знаки (русск.)
Банковский счет (англ.)	План развития компании (русск.)
Банковский счет (русск.)	План развития рынка (русск.)
Безопасность (англ.)	Платежи (англ.)
Бизнес-встречи и командировки (англ.)	Поиск работы (англ.)
Бизнес-встречи и командировки (русск.)	Прайс-листы (англ.)
Бизнес-документация (англ.)	Прибыли и убытки (англ.)
Бизнес-документация (русск.)	Прием, выписка (англ.)
Бизнес-документация: термины (англ.)	Прогнозы продаж (англ.)
Бизнес-документация: термины (русск.)	Проект: версии (русск.)
Бизнес-документация: типы (англ.)	Проект: даты выпуска (англ.)
Бизнес-документация: типы (русск.)	Проект: даты выпуска (русск.)
Бизнес-партнеры (русск.)	Проект: документация (русск.)
Бухгалтерская документация (русск.)	Проект: название (англ.)
Бухгалтерская документация: модели (англ.)	Проект: название (русск.)
Бухгалтерская документация: модели (русск.)	Производственные расходы (англ.)
Бухгалтерская документация: термины (англ.)	Производство (русск.)
Бухгалтерская документация: термины (русск.)	Профили (англ.)
Внутренние платежи (русск.)	Развитие компании (англ.)
Выписка по счету (русск.)	Развитие рынков (англ.)
Выплаты и премии (русск.)	Расистские высказывания (англ.)
Дата истечения (амер.)	Расистские высказывания (русск.)

Встроенные контентные группы ключевых слов

Дата рождения (амер.)	Распространенные заболевания (англ.)
Действующие вещества (англ.)	Расходы (русск.)
Дискредитирующая информация (англ.)	Резюме (англ.)
Документы ИТ отдела (русск.)	Сексуальные темы (англ.)
Документы отдела кадров (русск.)	Сетевая безопасность (англ.)
Журнал звонков сотового оператора (англ.)	Слияния и поглощения (англ.)
Закон о труде (русск.)	Собрание совета директоров (англ.)
Идентификатор плательщика федерального налога (амер.)	Социальное страхование (англ.)
Имя пользователя (англ.)	Спам (англ.)
Имя пользователя (русск.)	Спорт (англ.)
Инвестиции (англ.)	Страхование (русск.)
Инвесторы и инвестиции (русск.)	Тендерная документация (русск.)
Инновации (англ.)	Технологии (англ.)
Инновации (русск.)	Технологии (русск.)
Интернет аббревиатуры (англ.)	Увольнение (англ.)
Исходный код C#	Увольнение (русск.)
Исходный код C/C++	Употребление наркотических веществ (англ.)
Исходный код COBOL	Условия труда (англ.)
Исходный код Java	Условия труда (русск.)
Исходный код Perl	Физическая безопасность (русск.)
Исходный код VB	Финансовая выписка (англ.)
Компенсации и премии (англ.)	Финансовая информация (русск.)
Конкуренция (англ.)	Финансовые термины (русск.)
Конфиденциальная информация (русск.)	Финансовый отчет (англ.)
Конфиденциальная информация о партнерах (англ.)	Финансовый отчет (русск.)
Конфиденциально (англ.)	Цены (англ.)
Корпоративная собственность (русск.)	Цены (русск.)
Корпоративная юридическая документация (русск.)	

Создание пользовательских групп ключевых слов

Контентно-зависимые правила можно создавать на основе собственных (пользовательских) контентных групп, если предопределенные (встроенные) контентные группы не отвечают вашим нуждам. Пользовательские группы ключевых слов позволяют задавать любые ключевые слова и фразы внутри одной контентной группы, чтобы наилучшим образом решить задачи организации.

Чтобы создать пользовательскую группу ключевых слов

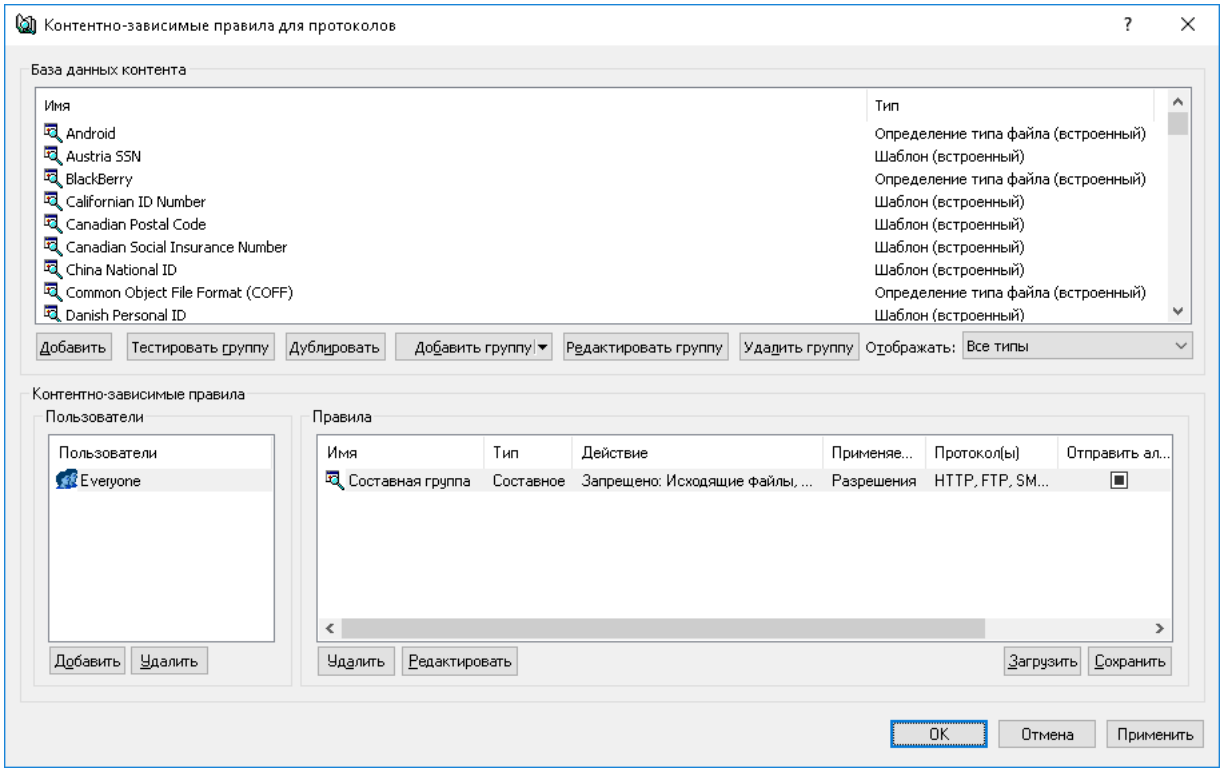
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства** либо узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

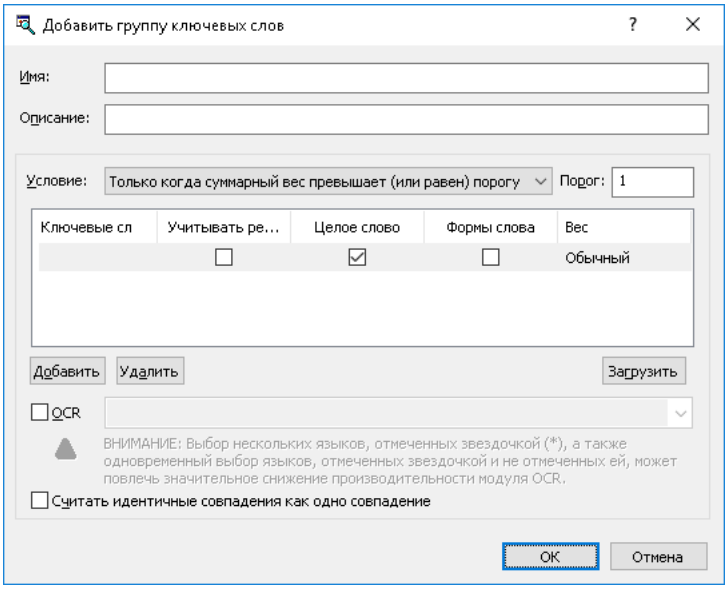
     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

Появится диалоговое окно, подобное приведенному ниже.



4. В верхней части появившегося диалогового окна в области **База данных контента** нажмите стрелку рядом с полем **Добавить группу**, а затем выберите пункт **Ключевые слова**.

   Появится диалоговое окно "Добавить группу ключевых слов".



5. В диалоговом окне **Добавить группу ключевых слов** выполните следующее:
    - **Имя** - Указать имя группы.
    - **Описание** - Указать описание группы.
    - **Условие** - Задать условия срабатывания правил, созданных на основе этой контентной группы. Для этого в списке **Условие** выберите один из следующих пунктов:
        - **Совпадение по любым ключевым словам** - Означает, что правило, основанное на этой контентной группе, срабатывает каждый раз, когда любое из заданных ключевых слов и фраз встречается в тексте.
        - **Совпадение по всем ключевым словам** - Означает, что правило, основанное на этой контентной группе, срабатывает каждый раз, когда все заданные ключевые слова и фразы встречаются в тексте.
        - **Только когда суммарный вес превышает (или равен) порогу** - Означает, что правило, основанное на этой контентной группе, срабатывает каждый раз, когда общее число (сумма) вхождений всех заданных ключевых слов и фраз будет больше или равно заданному пороговому числу вхождений ключевых слов.
    - **Порог** - Задать пороговое число вхождений ключевых слов. Это значение может быть установлено в диапазоне от 0 до 65535. Этот параметр должен быть установлен, если выбрано условие срабатывания **Только когда суммарный вес превышает (или равен) порогу**.
    - **Ключевые слова** - Задать слова и фразы, наличие которых будет проверяться в текстовых данных. Дважды щелкните в области **Ключевые слова**, чтобы ввести слово или фразу.
    - **Учитывать регистр** - Задать чувствительность ключевых слов к регистру. Установите флажок **Учитывать регистр**, чтобы задать чувствительное к регистру сравнение ключевых слов (например, слова `тест` и `Тест` будут рассматриваться как разные слова).

      Снимите флажок **Учитывать регистр**, чтобы задать не чувствительное к регистру сравнение ключевых слов (например, слова `тест` и `Тест` будут рассматриваться как одинаковые слова).
    - **Целое слово** - Задать параметры соответствия ключевым словам. Установите флажок **Целое слово**, чтобы задать строгое соответствие (позволяет находить точное совпадение с ключевым словом).

      Снимите флажок **Целое слово**, чтобы задать широкое соответствие (позволяет находить ключевое слово в различных грамматических вариациях).

- **Формы слова** - Обеспечивает морфологический поиск, учитывающий различные грамматические формы ключевых слов. Установите этот флажок, чтобы включить морфологический поиск на каталонском, английском, французском, немецком, итальянском, польском, португальском, русском и испанском языках. Кроме того, если этот флажок установлен, обеспечивается поиск русских слов, записанных латинскими буквами посредством транслитерации, а также поиск с учетом возможной замены некоторых символов другими, похожими по внешнему виду или значению, такими как:

  - Латинские буквы в русском тексте (например, латинская буква b вместо русской буквы ь)
  - Латинские буквы вместо некоторых цифр (например, латинская буква S вместо цифры 5)
  - Русские буквы в английском тексте (например, русская буква п вместо латинской буквы n)
  - Русские буквы вместо некоторых цифр (например, русская буква З вместо цифры 3)
  - Некоторые символы вместо русских букв (например, символ * (звездочка) вместо русской буквы ж)
  - Цифры вместо некоторых латинских или русских букв (например, цифра 1 вместо латинской буквы I или цифра 4 вместо русской буквы Ч)
  - Индо-арабские (восточно-арабские) цифры вместо обычных арабских цифр (например, символ ٣ вместо цифры 3 или символ ٨ вместо цифры 8)

  Морфологический поиск может занять много времени и ресурсов.

  Снимите флажок **Формы слова** для поиска ключевых слов без учета морфологии, транслитерации и подмены символов.

- **Вес** - Определить степень важности каждого ключевого слова или фразы. Степень важности (вес) используется для подсчета вхождений ключевых слов в тексте. Этот параметр должен быть установлен, если выбрано условие срабатывания **Только когда суммарный вес превышает (или равен) порогу**.

  Возможные значения: **Тяжелый**, **Выше обычного**, **Обычный** (значение по умолчанию), **Ниже обычного**, **Легкий**. Эти значения веса интерпретируются следующим образом:

  - **Тяжелый** - Означает, что каждое вхождение ключевого слова или фразы считается как три вхождения. Это самое высокое значение веса.
  - **Выше обычного** - Означает, что каждое вхождение ключевого слова или фразы считается как два вхождения.
  - **Обычный** - Означает, что каждое вхождение ключевого слова или фразы считается как одно вхождение.
  - **Ниже обычного** - Означает, что два вхождения ключевого слова или фразы считаются как одно вхождение.
  - **Легкий** - Означает, что три вхождения ключевого слова или фразы считаются как одно вхождение. Это самое низкое значение веса.

- **Добавить** - Задать ключевые слова и фразы. Нажмите кнопку **Добавить**, чтобы ввести ключевое слово или фразу.
- **Удалить** - Удалить ключевое слово. Для этого выберите ключевое слово, которое необходимо удалить, и затем нажмите кнопку **Удалить**.

  Чтобы выбрать одновременно несколько ключевых слов, используйте клавиши SHIFT или CTRL.
- **Загрузить** - Импортировать список ключевых слов из текстового файла. Каждое ключевое слово в этом файле должно располагаться на отдельной строке с переходом на новую строку после последнего символа ключевого слова.
- **OCR** - Извлекать текст из изображений для его последующей проверки по ключевым словам этой контентной группы. Установите флажок **OCR** и выберите не более 8 языков, чтобы включить распознавание.

  Примечание: Выбор нескольких азиатских языков (отмеченных звездочкой (*) в пользовательском интерфейсе), а также одновременный выбор азиатских и не азиатских языков может повлечь значительное снижение производительности модуля OCR.

  Для достижения оптимальной производительности и точности распознавания рекомендуется выбирать минимально необходимое количество языков.
- **Считать идентичные совпадения как одно совпадение** - Объединить повторяющиеся результаты обнаружения ключевого слова в один результат. Для этого установите **Считать идентичные совпадения как одно совпадение**. Этот параметр доступен, если выбрано условие срабатывания **Только когда суммарный вес превышает (или равен) порогу**.

6. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Добавить группу ключевых слов**.

   Новая контентная группа добавляется в список существующих контентных групп в области "База данных контента" в верхней части диалогового окна для управления контентно-зависимыми правилами.

Группы шаблонов

Группы шаблонов позволяют контролировать доступ к текстовым файлам, используя шаблоны регулярных выражений Perl. Шаблоны предоставляют гибкий и мощный способ автоматически находить потенциально важные данные в документах (например, номера кредитных карт, номера СНИЛС, адреса электронной почты и телефонные номера).

Для получения подробной информации о создании и использовании регулярных выражений на языке Perl обратитесь к руководствам "Perl regular expressions quick start" по адресу perldoc.perl.org/perlrequick.html и "Perl regular expressions tutorial" по адресу perldoc.perl.org/perlretut.html.

DeviceLock предоставляет более 75 предопределенных (встроенных) групп шаблонов, которые можно использовать для настройки прав доступа и/или операций теневого копирования. Можно использовать встроенные группы "как есть", создавать их редактируемые копии (дубликаты) или создавать собственные группы, необходимые для решения частных задач организации.

Встроенные группы облегчают задачу настройки контентно-зависимых правил, позволяя во многих случаях обойтись без создания пользовательских групп.

Примечание: Имеется возможность просмотра параметров любой встроенной группы, однако изменять параметры встроенных групп или удалять такие группы невозможно. Подробнее см. в разделе Просмотр встроенных контентных групп.

В следующей таблице перечислены все встроенные группы данного типа:

Встроенные контентные группы шаблонов

Californian ID Number	Адрес (русск.)
Canadian Postal Code	Адрес электронной почты
Canadian Social Insurance Number	Американские имена (англ.)
China National ID	БИК (ISO 9362)
Danish Personal ID	БИК (русск.)
Dominican Republic ID Number	Болгарский: ЕГН
Finnish ID	Время (12/24 формат)
France INSEE Code	ГРЗ автомобиля (русск.)
French NINO	ГРЗ мотоцикла (русск.)
German eTIN	ГРЗ прицепа (русск.)
GPS-данные (RMC-строка)	Дамп кредитных карт
Health Insurance Claim	Дата (ISO)
IBAN-номер	Дата (амер.)
IP-адрес	Европейский номер плательщика НДС
Irish PPSN	ИНН (русск.)
Irish VAT	Ключ продукта Microsoft Windows
Japan: Address	Код подразделения, выдавшего паспорт (русск.)
Japan: Date	Корреспондентский счет (русск.)
Japan: Phone Number	КПП (русск.)
Japan: Social Security and Tax Number System	Номер банковского счета (русск.)

Встроенные контентные группы шаблонов

MAC-адрес	Номер водительского удостоверения (русск.)
Mexican Tax Id Number	Номер дипломатического паспорта (русск.)
National Provider Identifier	Номер заграничного паспорта (русск.)
Norwegian Birth Number	Номер карточки социального страхования (амер.)
Poland National Identity Card Number	Номер кредитной карты
Polish ID Number	Номер ОСАГО (русск.)
RAMQ	Номер паспорта (русск.)
Scotland CHI	Номер паспорта гражданина СССР
South African Id Number	Номер полиса ОМС (русск.)
South Korean Resident Registration Number	Номер порта TCP/UDP
Spanish DNI	Номер свидетельства о регистрации ТС (русск.)
Spanish Full Name	Номер телефона (Америка)
Spanish NIF	Номер телефона (Германия)
Spanish SSN	Номер телефона (Россия)
SQL-запросы	Номер телефона (международный)
Sweden Personal ID	Номер трудовой книжки (русск.)
Sweden Phone Number	ОГРН (русск.)
Taiwan: ID Number	ОГРНИП (русск.)
Taiwan: Jih Sun Bank Account Number	ОКАТО (русск.)
Turkish ID Number	ОКВЭД (русск.)
UK Date	ОКОГУ (русск.)
UK National Insurance Number	ОКОПФ (русск.)
UK NHS Number	ОКПО (русск.)
UK Phone Number	ОКФС (русск.)
UK RD&E Hospital Number	Почтовый индекс (Великобритания)
UK Tax Code	Почтовый индекс (Россия)
URL-адрес	Почтовый индекс (США)
US/UK Home Address	Почтовый индекс (Швеция)
VIN-номер автомобиля	СНИЛС (русск.)
ABA-номер	Социальная карта (русск.)
Австрийский SSN	Цена в долларах (англ.)

Создание пользовательских групп шаблонов

Контентно-зависимые правила можно создавать на основе собственных (пользовательских) контентных групп, если предопределенные (встроенные) группы не отвечают вашим нуждам. Пользовательские группы шаблонов позволяют задавать любой шаблон регулярного выражения для поиска нужной информации в текстовых данных.

Чтобы создать пользовательскую группу шаблонов

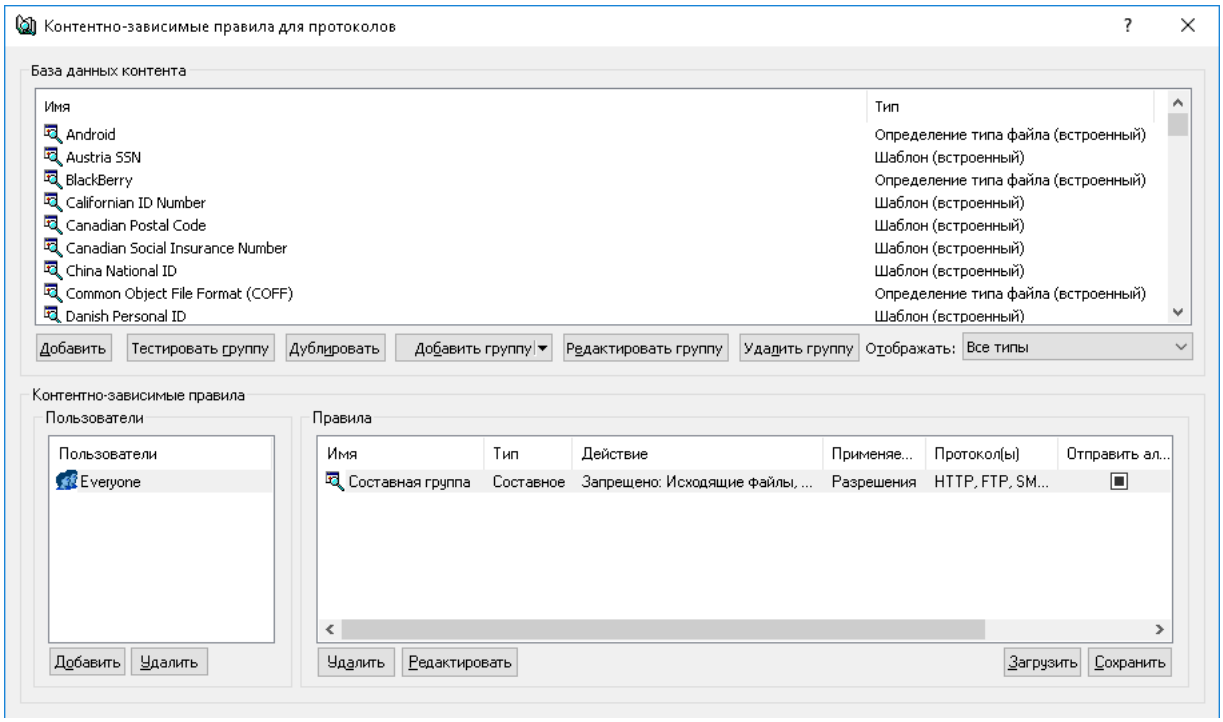
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства** либо узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

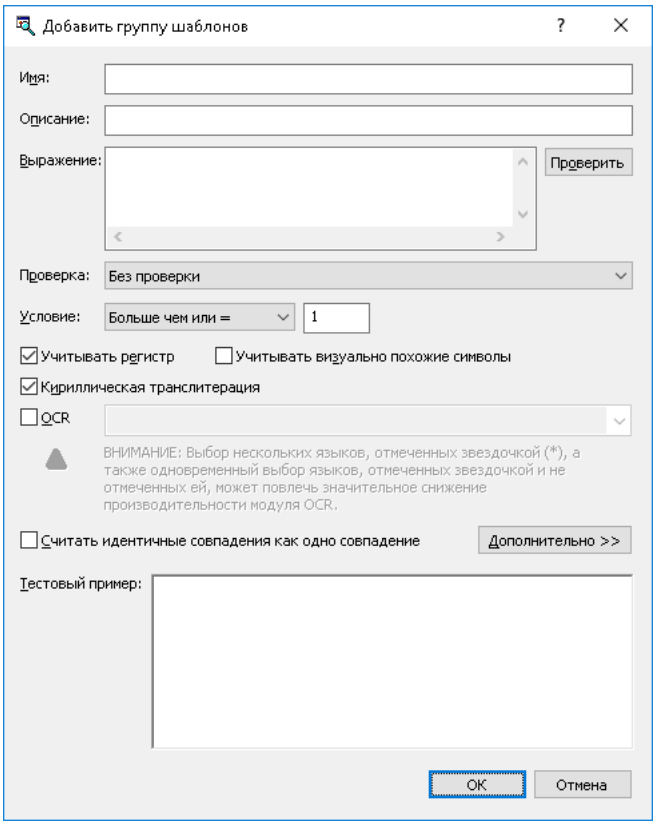
     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно, подобное приведенному ниже.



4. В верхней части появившегося диалогового окна в области **База данных контента** нажмите стрелку рядом с полем **Добавить группу**, а затем выберите пункт **Шаблон**.

   Появится диалоговое окно "Добавить группу шаблонов".



5. В диалоговом окне **Добавить группу шаблонов** выполните следующее:
   - **Имя** - Указать имя группы.
   - **Описание** - Указать описание группы.
   - **Выражение** - Задайте шаблон, указав одно или несколько регулярных выражений Perl, по одному выражению на строку. Соответствие данных группе обнаруживается в случае их соответствия любому из указанных выражений. Подробнее о регулярных выражениях см. в руководствах "Perl regular expressions quick start" по адресу perldoc.perl.org/perlrequick.html и "Perl regular expressions tutorial" по адресу perldoc.perl.org/perlretut.html.
   - **Проверить** - Проверить синтаксис регулярного выражения.

- **Проверка** - Если настроена проверка, то соответствие данных группе обнаруживается только в случае их соответствия выбранному типу проверки. Чтобы соответствовать группе, данные должны соответствовать регулярному выражению, а также пройти проверку.

  Если для этого поля выбран вариант **Без проверки**, то для соответствия данных группе достаточно их соответствия регулярному выражению.

  Чтобы настроить проверку, выберите нужный тип из выпадающего списка в этом поле. Предусмотрены следующие типы проверки: **HIC**, **IBAN**, **ID Доминиканской республики**, **IP-адрес**, **NPI**, **URL**, **Австрийский SSN**, **Адрес e-mail**, **Американское имя (Ex)**, **Болгарский ЕГН**, **Дамп кредитных карт**, **Дата**, **Дата (ISO)**, **Датский персональный ID**, **Европейские номер VAT**, **Ирландский PPSN**, **Испанский NIF**, **Квебекский номер мед. страховки**, **Китайский национальный ID**, **Контрольная сумма LUHN**, **Мексиканский Id налогоплательщика**, **Немецкий eTIN**, **Номер UK NHS**, **Номер кредитной карты (American Express)**, **Номер кредитной карты (Carte Blanche)**, **Номер кредитной карты (Diners Club)**, **Номер кредитной карты (Discover)**, **Номер кредитной карты (En Route)**, **Номер кредитной карты (JCB)**, **Номер кредитной карты (Laser)**, **Номер кредитной карты (Maestro)**, **Номер кредитной карты (Master Card)**, **Номер кредитной карты (Solo)**, **Номер кредитной карты (Switch)**, **Номер кредитной карты (Visa Electron)**, **Номер кредитной карты (Visa)**, **Номер кредитной карты (Все)**, **Номер кредитной карты (МИР), Номер маршрутизации ABA**, **Номер налогоплательщика UK**, **Номер соц. страхования (Канада)**, **Номер соц. страхования (США)**, **Номер социального страхования UK**, **Норвежский номер рождения**, **Основной Государственный Регистрационный Номер**, **Польская карта идентификации**, **Польский ID**, **Почтовый индекс UK**, **Российская классификация предприятий и организаций**, **Российский код подразделения, выдавшего паспорт**, **Российский КПП**, **Российский номер банковского счета**, **Российский номер корреспондентского счета**, **Российский номер налогоплательщика**, **Российский номер социального страхования**, **Российский номер социальной карты**, **Российский ОГРНИП**, **Российский ОКАТО**, **Российский ОКОГУ**, **Российский ОКОПФ**, **Российский ОКФС**, **Российский СНИЛС**, **Тайваньский ID**, **Телефон (UK)**, **Турецкий номер Id**, **Финский ID**, **Французский код INSEE**, **Южно-африканский Id налогоплательщика**, **Южно-корейский номер регистрации**, **Японский номер соц. страхования и ID-налогоплательщика**.

- **Условие** - Выбрать условие срабатывания правил проверки контента, использующих данную группу:

  - **Меньше чем или =** - Правило срабатывает, если обнаружено не более заданного числа совпадений с регулярным выражением.
  - **Равно** - Правило срабатывает, если количество обнаруженных совпадений с регулярным выражением равно заданному числу.
  - **Больше чем или =** - Правило срабатывает, если обнаружено не менее заданного числа совпадений с регулярным выражением.
  - **Между** - Правило срабатывает, если количество обнаруженных совпадений с регулярным выражением находится в заданном диапазоне.
  - **Точное совпадение** - Правило срабатывает, если весь предоставленный на проверку контент соответствует регулярному выражению.

    Внимание: На точное совпадение проверяется не более первого мегабайта из предоставленного на проверку контента. Если этот контент превышает 1 МБ, правило с условием **Точное совпадение** не срабатывает, даже если первый мегабайт соответствует регулярному выражению группы.

Примечание: Если выбрано условие **Точное совпадение**, группа обнаруживает совпадение, когда весь проверяемый контент соответствует ее регулярному выражению. Как следствие, правило проверки срабатывает только при условии, что регулярное выражение соответствует всей последовательности символов, составляющих данный контент.

При любом условии, отличном от опции **Точное совпадение**, группа выполняет поиск последовательности символов, соответствующей данному регулярному выражению. Совпадение обнаруживается, если где-либо в проверяемом контенте есть последовательность символов, которая соответствует этому выражению.

- **Учитывать регистр** - Если этот флажок установлен, группа различает строчные и прописные буквы. Например, слова `Серия` и `серия` будут обрабатываться по-разному, что позволяет настроить группу так, чтобы ей соответствовало слово `Серия`, но не `серия`.

  Когда этот флажок снят, группа не проводит различия между прописными и строчными буквами. Например, если данной группе соответствует слово `Серия`, то ей будут соответствовать также слово `серия` и даже слово `сЕрИя`.

- **Учитывать визуально похожие символы** - Если этот флажок установлен, группа обнаруживает данные, которые соответствуют ее выражению, даже в случае замены отдельных символов на другие, сходные по внешнему виду или значению, в том числе:

  - Латинские буквы в русском тексте (например, латинская буква `b` вместо русской буквы `ь`)
  - Латинские буквы вместо некоторых цифр (например, латинская буква `S` вместо цифры `5`)
  - Русские буквы в английском тексте (например, русская буква `п` вместо латинской буквы `n`)
  - Русские буквы вместо некоторых цифр (например, русская буква `З` вместо цифры `3`)
  - Некоторые символы вместо русских букв (например, символ `*` (звездочка) вместо русской буквы `ж`)
  - Цифры вместо некоторых латинских или русских букв (например, цифра `1` вместо латинской буквы `I` или цифра `4` вместо русской буквы `Ч`)
  - Индо-арабские (восточно-арабские) цифры вместо обычных арабских цифр (например, символ `٣` вместо цифры `3` или символ `٨` вместо цифры `8`)

  Когда этот флажок снят, группа строго различает символы независимо от того, похожи они или нет по внешнему виду или значению.

- **Кириллическая транслитерация** - Если этот флажок установлен, группа распознает кириллический текст, подлежащий обнаружению, независимо от того, написан ли текст кириллицей или латинскими буквами. Например, если слово `Серия` соответствует данной группе, то ей будет соответствовать также слово `Seriya`.

  Когда этот флажок снят, соответствие текста группе строго зависит от алфавита, используемого для написания текста. Например, группу можно настроить так, чтобы ей соответствовало слово `Серия`, но не `Seriya`.

- **OCR** - Извлекать текст из изображений для его последующей проверки регулярным выражением этой контентной группы. Установите флажок **OCR** и выберите не более 8 языков, чтобы включить распознавание.

  Примечание: Выбор нескольких азиатских языков (отмеченных звездочкой (*) в пользовательском интерфейсе), а также одновременный выбор азиатских и не азиатских языков может повлечь значительное снижение производительности модуля OCR.

  Для достижения оптимальной производительности и точности распознавания рекомендуется выбирать минимально необходимое количество языков.

- **Считать идентичные совпадения как одно совпадение** - Объединить повторяющиеся результаты, возвращенные регулярным выражением, в один результат. Для этого установите флажок **Считать идентичные совпадения как одно совпадение**.

- **Дополнительно** - Быстро проверить шаблон регулярного выражения на пробном тексте. Нажмите кнопку **Дополнительно**, чтобы показать или скрыть поле **Тестовый пример**.

- **Тестовый пример** - Ввести текстовую строку для проверки соответствия шаблону и просмотреть результат. DeviceLock выделяет цветом результаты проверки в режиме реального времени. Все совпадения с шаблоном выделяются зеленым цветом, а строки, не совпадающие с шаблоном, выделяются красным цветом.

6. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Добавить группу шаблонов**.

   Новая контентная группа добавляется в список существующих контентных групп в области "База данных контента" в верхней части диалогового окна для управления контентно-зависимыми правилами.

Группы свойств документа

Группы свойства документа предназначены для контроля доступа к файлам на основании их свойств: имени файла, размера и т.д. Также с их помощью можно контролировать доступ к защищенным паролем документам и архивам, а также изображениям, содержащим текст.

Примечание: Логика "И" применяется для всех свойств файла, заданных в группе свойств документа. Например, если требуется контролировать доступ к файлам больше 5 мегабайт (МБ) и защищенные паролем документы и архивы, следует создать две отдельные группы свойств документа: одна группа для файлов размером более 5 МБ, а другая группа для защищенных паролем документов и архивов. Если задать указанные свойства в одной группе, а затем создать на основе этой группы контентно-зависимое правило, то данное правило будет контролировать защищенные паролем документы и архивы размером более 5 МБ.

DeviceLock не предоставляет встроенных групп свойств документа. Следующая процедура описывает, как создать собственную группу свойства документа.

Чтобы создать группу свойств документа

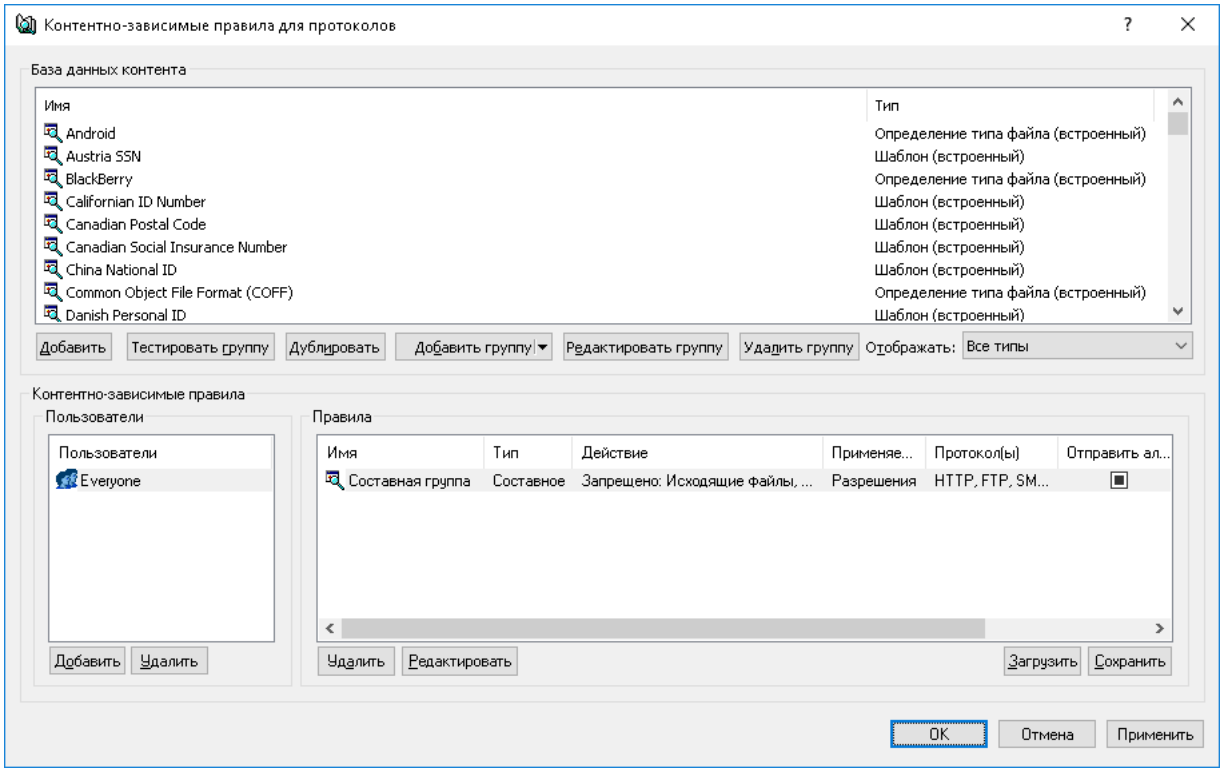
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства** либо узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

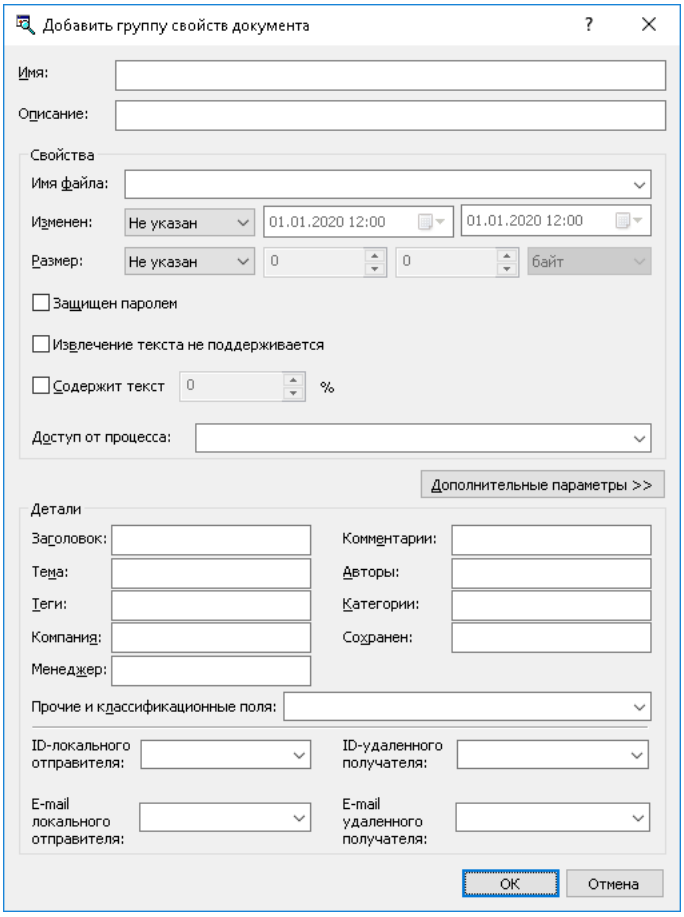
     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

Появится диалоговое окно, подобное приведенному ниже.



4. В верхней части появившегося диалогового окна в области **База данных контента** нажмите стрелку рядом с полем **Добавить группу**, а затем выберите пункт **Свойства документа**.

Появится диалоговое окно “Добавить группу свойств документа”.



5. В диалоговом окне **Добавить группу свойств документа** выполните следующие действия:

   - **Имя** - Указать имя группы.
   - **Описание** - Указать описание группы.
   - **Имя файла** - Задать имена файлов. Можно использовать знаки подстановки, такие как * и ?. Звездочка (*) обозначает произвольную последовательность символов или их отсутствие. Например, `*.txt` соответствует любому имени файла с расширением `txt`. Вопросительный знак (?) обозначает один произвольный символ. Например, `????.*` соответствует имени из любых 4-х символов с любым расширением. Если имен файлов несколько, их следует разделять точкой с запятой (;), например, `*.doc; *.docx`.

     Примечание: Для данных теневого копирования, полученных от типа устройств **Принтер**, заданное имя файла сравнивается с именами, представленными в столбце **Имя файла** просмотрщика журнала теневого копирования.

   - **Изменен** - Задать дату и время последнего изменения файла. Для этого выберите в списке **Изменен** один из следующих вариантов:
     - **Не указан** - При анализе содержимого файла дата и время его последнего изменения не учитываются. Этот вариант выбран по умолчанию.
     - **До** - Дата и время последнего изменения файла должны быть раньше заданной даты/времени.

- **После** - Дата и время последнего изменения файла должны быть позже заданной даты/времени.
- **Между** - Дата и время последнего изменения файла должны быть в заданном диапазоне значений даты/времени.
- **Не старше чем** - Дата и время последнего изменения файла должны быть не позже заданного числа секунд, минут, часов, дней, недель, месяцев или лет.
- **Старше чем** - Дата и время последнего изменения файла должны быть позже заданного числа секунд, минут, часов, дней, недель, месяцев или лет.

Примечание: Параметр **Изменен** не действует в случае передачи файлов по сети. При анализе содержимого файлов, передаваемых по сети, дата и время их изменения не учитывется.

- **Размер** - Задать размер файла в байтах, килобайтах, мегабайтах, гигабайтах или терабайтах. Для этого выберите в списке **Размер** один из следующих вариантов:
  - **Не указан** - При анализе содержимого файла его размер не учитывается. Этот вариант выбран по умолчанию.
  - **Равен** - Размер файла должен быть равен заданному значению.
  - **Меньше чем** - Размер файла должен быть не больше заданного значения.
  - **Больше чем** - Размер файла должен быть не меньше заданного значения.
  - **Между** - Размер файла должен находиться в заданном промежутке.
- **Защищен паролем** - Позволяет данной группе обнаруживать и контролировать защищенные паролем архивы, PDF-файлы, документы Microsoft Office (.doc, .xls, .ppt, .vsd, .docx, .xlsx, .pptx, .vsdx) и документы AutoCAD 2012 (файлы .dwg).

  Когда у группы установлен флажок **Защищен паролем**, основанные на этой группе правила обнаруживают и контролируют архивы и другие поддерживаемые типы файлов, в которых пароль используется для ограничения доступа к файлу и/или его содержимому. Список поддерживаемых архивов см. в описании функции Проверка файлов внутри архивов.

  При использовании контентно-зависимых правил считается, что файл защищен паролем только в следующих случаях:

  - Для открытия данного файла требуется пароль.
  - Для доступа к некоторым вложениям в данном файле требуется пароль.
  - Данный файл содержит другие файлы, защищенные паролем.

    В последних двух случаях должен быть включен параметр Проверка содержимого архивов при чтении или Проверка содержимого архивов при записи, иначе DeviceLock не будет считать, что данный файл защищен паролем.

  Правила, основанные на группе, у которой флажок **Защищен паролем** не установлен, не учитывают парольную защиту проверяемых файлов.

  Примечание: Разрешающее правило, основанное на группе, у которой установлен флажок **Защищен паролем**, имеет приоритет над запрещающими правилами, разрешая передачу любого соответствующего этому правилу контента. Разрешающее правило, основанное на составной группе, будет иметь приоритет в том случае, когда логически связанная цепочка групп, разрешающая данный контент, имеет в своем составе группу, у которой установлен флажок **Защищен паролем**.

- **Извлечение текста не поддерживается** - Позволяет контролировать доступ к файлам, формат которых не поддерживается. Если этот флажок установлен для группы свойств документа и на ее основе создано контентно-зависимое правило, это правило будет контролировать доступ ко всем файлам, формат которых не поддерживается в механизмах контентного анализа DeviceLock. Все поддерживаемые форматы файлов перечислены в разделе Модули ContentLock и NetworkLock (см. Поддержка множества типов файлов и данных).

  Флажок **Извлечение текста не поддерживается** позволяет контролировать передачу разделенных на несколько частей (многотомных) архивов .cab или .rar, которые не могут быть распакованы и проанализированы по умолчанию, когда заданы контентно-зависимые правила и включены параметры **Проверка содержимого архивов при чтении** или **Проверка содержимого архивов при записи**. Разрешающее контентно-зависимое правило на основе группы свойств документа с установленным флажком **Извлечение текста не поддерживается** имеет приоритет над запрещающими правилами, позволяя передавать любой подходящий под это правило контент, в том числе части многотомных архивов.

- **Содержит текст** <число> **%** - Обнаруживать и контролировать доступ к графическим изображениям, содержащим текст. Если установлен флажок **Содержит текст** для группы свойств документа и создано сложное контентно-зависимое правило на основе этой контентной группы и встроенной контентной группы определения типа файла **Изображения, чертежи, CAD**, связанных оператором AND, это правило будет проверять, содержит ли графическое изображение поддерживаемого формата текст, и контролировать доступ к изображениям, которые содержат текст. Снимите флажок **Содержит текст**, если не требуется обнаруживать и контролировать доступ к изображениям, содержащим текст. Перечень поддерживаемых типов файлов изображения см. в разделе Обнаружение текста на изображении.

  Если флажок **Содержит текст** установлен, нужно указать количество текста на изображении в процентах от всей области изображения. Например, если текст занимает половину изображения, количество текста составляет 50%. Если изображение состоит только из текста, то количество текста составляет 100%.

  Примечание: Параметр **Содержит текст** применяется и к другим форматам файлов (см. Поддержка множества типов файлов и данных). В этом случае процентное содержание текста означает соотношение объема текста в символах к размеру файла в байтах.

- **Доступ от процесса** - Задать имя процесса, который получает доступ к файлу. Можно использовать знаки подстановки, такие как звездочка (*) и знак вопроса (?). Если процессов несколько, их имена следует разделять точкой с запятой (;), например, `explorer.exe; notepad.exe`.

- **Дополнительные параметры** - Позволяют настроить группу для распознавания различных свойств проверяемых документов, таких как встроенные и настраиваемые (пользовательские) свойства документов Microsoft Office и документов других типов, отправителей и получателей мгновенных сообщений и электронных писем, а также метки классификации, применяемые сторонними продуктами, такими как Boldon James Classifier.

  При использовании дополнительных параметров учитывайте следующее:

  - Различные параметры объединяются по И, то есть группа распознает документ, если он соответствует каждому из настроенных параметров. Например, чтобы документ распознавался группой, у которой заданы значения параметров `Заголовок` и `Тема`, соответствующие значения должны быть как у свойства `Заголовок`, так и у свойства `Тема` документа. Если требуется объединить параметры по ИЛИ, можно использовать составную группу, добавив в нее по отдельной группе свойств документа для каждого параметра.
  - Для одного и того же параметра можно задать несколько значений, разделяя их точкой с запятой. В таком случае значения объединяются по ИЛИ, так что группа распознает документ, если он соответствует любому из заданных значений. Так, если в параметре `Заголовок` указано `Отчет; Счет`, то группа распознает документы, у которых в свойстве `Заголовок` значится `Отчет` или `Счет`.

  Предусмотрены следующие дополнительные параметры:

  - **Заголовок**, **Тема**, **Теги**, **Компания**, **Менеджер**, **Комментарии**, **Авторы**, **Категории**, **Сохранен** - Эти поля служат для ввода значений, которые отвечают некоторым часто используемым свойствам документов, подлежащих контролю. Поддерживаются свойства документов MS Office (.docx, .xlsx, .pptx, .vsdx), .pdf и составных документов. Заголовок поля соответствует имени свойства, указанному в приложениях для работы с документами (например, MS Office Word или Adobe Acrobat).

    Допускается использование знаков подстановки: звездочка (*) обозначает произвольную группу символов или их отсутствие; вопросительный знак (?) обозначает один произвольный символ. Нескольких значений в одно и то же поле можно ввести, разделяя их точкой с запятой (;). Пример ввода двух значений с подстановочными символами: `*Отчет*; *Счет*`.

    Значения, введенные в разных полях, объединяются по И. Если в одном поле введено несколько значений, они объединяются по ИЛИ.

  - **Прочие и классификационные поля** - Это поле можно использовать для ввода значений, которые отвечают различным встроенным и настраиваемым (пользовательским) свойствам документов, подлежащих контролю. Поддерживаются свойства документов MS Office (.docx, .xlsx, .pptx), .pdf и составных документов.

    Чтобы ввести одно значение для некоторого свойства, используйте следующий синтаксис: `<имя свойства>=<значение свойства>`. Например, запись `Division=Sales` представляет значение Sales для свойства Division. Чтобы ввести несколько значений для одного и того же свойства, разделите их запятой. В этом случае значения объединяются по ИЛИ. Так, запись `Division=Sales,Finance` представляет значение Sales ИЛИ значение Finance для свойства Division.

    Чтобы ввести значения для нескольких свойств, разделите записи свойств точкой с запятой. Пример: `<имя1>=<значение11>,<значение12>; <имя2>=<значение21>`. Значения различных свойств объединяются по И, тогда как различные значения одного и того же свойства объединяются по ИЛИ. Так, запись `Division=Sales,Finance; Office=Head Office` представляет значение Sales ИЛИ значение Finance для свойства Division И значение Head Office для свойства Office.

Поле **Прочие и классификационные поля** позволяет также настроить группу для распознавания классификационных меток сторонних продуктов, таких как Boldon James Classifier, которые сохраняют значения своих меток в свойствах документа. Если меткой является точное значение некоторого свойства, то для ее распознавания можно использовать описанный выше синтаксис `<имя свойства>=<значение свойства>`. Какое именно значение какого свойства служит для обозначения метки определяется настройками стороннего продукта.

Чтобы настроить группу для распознавания SISL-меток Boldon James Classifier, используется синтаксис, который указывает идентификатор элемента `uid` требуемой метки: `uid=<значение ID>`. Значение ID можно выяснить из XML-данных SISL-метки какого-либо классифицированного документа. Подробнее об этом см. в разделе Распознавание меток Boldon James Classifier.

В поле **Прочие и классификационные поля** можно использовать точку с запятой (;) в качестве разделителя для ввода нескольких записей, обозначающих различные свойства документа и/или классификационные метки. Все записи, разделенные точкой с запятой, объединяются по И.

> **Примечание:** Для облегчения настройки группы в поле **Прочие и классификационные поля** запоминаются ранее вводившиеся записи с возможностью их выбора из раскрывающегося списка, которым снабжено это поле.

- **ID-локального отправителя**, **ID-удаленного получателя** - Эти поля служат для ввода идентификаторов локальных отправителей и/или идентификаторов удаленных получателей мгновенных сообщений, подлежащих контролю. Используйте запятую (,) или точку с запятой (;) для разделения идентификаторов в строке. Можно использовать знаки подстановки (* и ?).

> **Примечание:** Параметры ID-локального отправителя и ID-удаленного получателя применимы только к протоколам. В контентно-зависимых правилах для устройств эти параметры не действуют.

Идентификаторы пользователей могут быть указаны для следующих протоколов: ICQ Messenger, Jabber, Mail.ru Агент, Skype, Telegram, Viber, WhatsApp, Zoom.

Пользователи ICQ Messenger идентифицируются по номеру UIN (например, `111222`, `23232323`).

Пользователи Jabber идентифицируются по Jabber ID в следующем формате: `<user>@<domain>`

Пользователи Mail.ru Агента идентифицируются по адресу электронной почты в следующем формате: `<user>@mail.ru`

Пользователи Skype, Telegram, Viber, WhatsApp или Zoom идентифицируются по соответствующему ID пользователя.

- **E-mail локального отправителя**, **E-mail удаленного получателя** - Эти поля служат для ввода адресов локальных отправителей и/или адресов удаленных получателей электронных писем, подлежащих контролю. Используйте запятую (,) или точку с запятой (;) для разделения адресов в строке. Можно использовать знаки подстановки (* и ?).

  Примечание: Параметры **E-mail локального отправителя** и **E-mail удаленного получателя** применимы только к протоколам. В контентно-зависимых правилах для устройств эти параметры не действуют.

  Адреса электронной почты могут быть указаны для следующих протоколов: MAPI, SMTP, IBM Notes, Web-почта.

  Адрес электронной почты указывается в формате `<user>@<domain>` (или `<user>/<domain>` для IBM Notes). Чтобы указать группу адресов, используйте звездочку (*). Например, `*@domain.com` (или `*/domain` для IBM Notes) обозначает все адреса из указанного домена.

  Используя эти параметры в случае Web-почты, примите во внимание следующие соображения:

  - Проверка адреса отправителя и получателя для вложений, оправляемых по Web-почте, возможна только в момент отправки письма, а не в момент загрузки вложения на сервер Web-почты. Поэтому мы не рекомендуем использовать эти параметры при построении политики безопасности для пользователей Web-почты. По соображениям безопасности DeviceLock не позволяет выполнять загрузку почтовых вложений на сервер Web-почты, если правило, разрешающее отправку вложений по Web-почте, использует E-mail локального отправителя или E-mail удаленного получателя.
  - Правила, применимые для ограничения отправки писем по Web-почте, позволяют сохранять черновики писем, если те не содержат запрещенных отправителей и/или получателей, что позволит пользователям получить доступ к контенту извне и может привести к утечке данных. Создавать такие правила не рекомендуется.

При использовании параметров для указания отправителей или получателей учитывайте следующее:

- Для разрешения или запрета передачи определенного контента между определенными лицами мы рекомендуем применять составные группы, объединяющие по И группу свойств документа, которая указывает желаемых отправителей и/или получателей, с другими контентными группами (определения типа файла, ключевые слова и т.д.).

6. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Добавить группу свойств документа**.

   Новая контентная группа добавляется в список существующих контентных групп в области "База данных контента" в верхней части диалогового окна для управления контентно-зависимыми правилами.

Распознавание меток Boldon James Classifier

Группы свойств документа позволяют выполнять проверку контента с использованием меток, которые ставятся приложениями Boldon James Classifier на документах. Такую проверку можно реализовать, настроив группу на распознавание требуемых меток, а затем создавая контентно-зависимые правила на основе этой группы. Правила могут применяться как к устройствам, так и к сетевым протоколам, позволяя использовать метки Boldon James Classifier для управления разрешениями на доступ/передачу контента, контентно-зависимым созданием теневых копий и/или простым обнаружением контента.

У документов MS Office метки Boldon James Classifier сохраняются в свойствах документа. Когда на документе ставится метка, добавляется ряд новых свойств документа, содержащих данные метки. Эти свойства и их значения можно увидеть в стандартном диалоговом окне для просмотра свойств документа в приложениях MS Office. У большинства таких свойств в начале имени имеется префикс `bj`.

Метка может представлять собой точное значение некоторого свойства документа, например, `bjDocumentSecurityLabel`: `This information is Classified | Internal`. Чтобы настроить группу для распознавания подобной метки, можно применить следующий синтаксис в поле **Прочие и классификационные поля**: `<имя свойства>=<значение свойства>` (см. описание этого поля в разделе Группы свойств документа).

Boldon James Classifier также может представлять свои метки в виде данных XML, хранящихся в свойствах документа. Метки такого типа называются SISL-метками. Для документов MS Office данные SISL-меток хранятся в свойстве `bjDocumentLabelXML`. Часть строки XML данных SISL-метки может быть сохранена в дополнительном свойстве `bjDocumentLabelXML-0`.

Значением SISL-метки является ID элемента `uid` в ее XML данных. Значение ID может быть строковым или численным. Чтобы настроить группу для распознавания такой метки следует применить синтаксис, в котором указывается идентификатор элемента `uid` данной SISL-метки: `uid=<значение ID>` (см. описание поля Прочие и классификационные поля в разделе Группы свойств документа).

Например, в свойстве `bjDocumentLabelXML` документа MS Office могут встретиться следующие данные SISL-метки:

```
<?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>
```

Для распознавания этой метки введите следующую запись в поле **Прочие и классификационные поля**: `uid=id_classification_internalonly` (без кавычек).

Составные группы

Составные группы позволяют использовать логические выражения для более гибкого определения данных, подлежащих контролю. Эти группы могут содержать любую комбинацию встроенных или пользовательских контентных групп определения типа файла, ключевых слов, шаблонов, свойств документа и цифровых отпечатков, связанных стандартными логическими операторами. Каждая контентная группа рассматривается как отдельный критерий фильтра, включенный в логическое выражение. Используя несколько контентных групп, можно создавать сложные фильтры для обнаружения важной информации в данных, передаваемых по сети.

Следующая таблица содержит перечень логических операторов в порядке их приоритета от высшего к низшему.

Оператор	Значение
НЕ	Логическое отрицание
И	Должны применяться оба критерия фильтра
ИЛИ	Должен применяться один из критериев фильтра

Чтобы изменить приоритет операторов в выражении, следует использовать круглые скобки. Если в выражении содержатся вложенные скобки, то сначала вычисляется результат наиболее глубоко вложенных скобок. Поддерживается несколько уровней вложения. Составная группа может содержать не более 50 контентных групп.

DeviceLock не предоставляет встроенных составных групп. Следующая процедура описывает, как создать собственную составную группу.

Чтобы создать составную группу

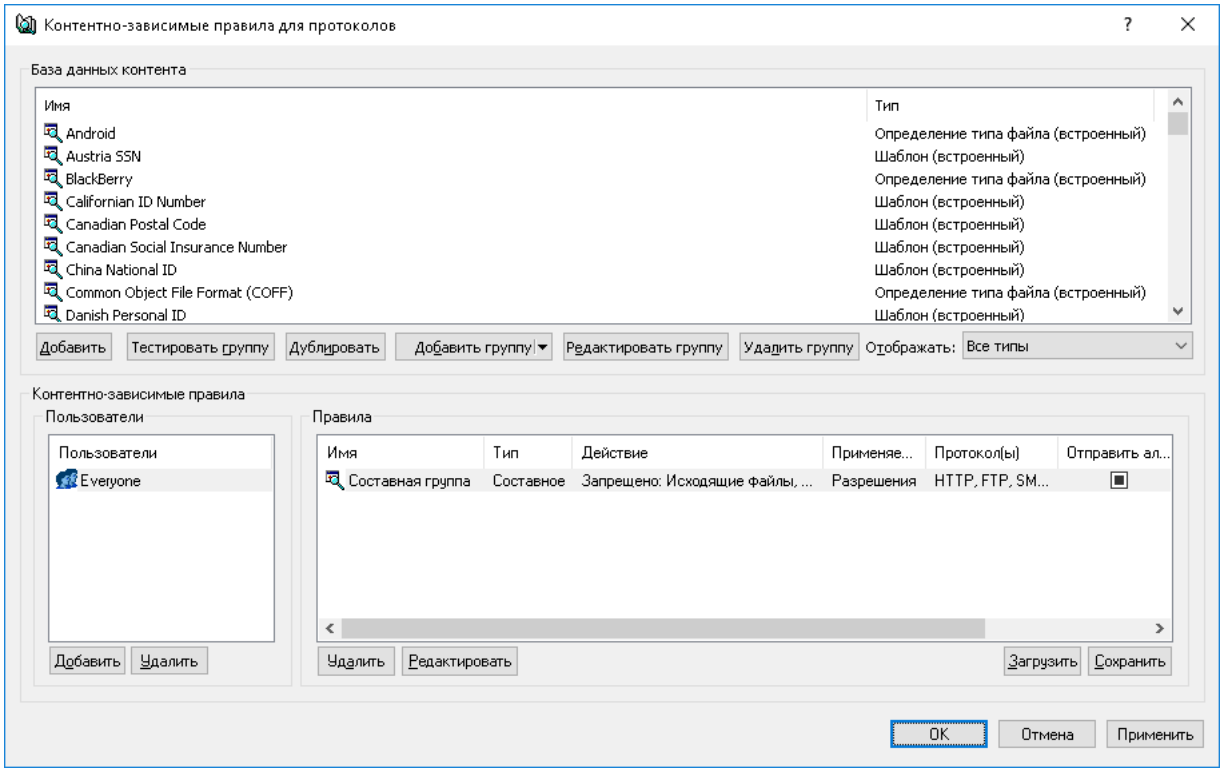
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства** либо узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

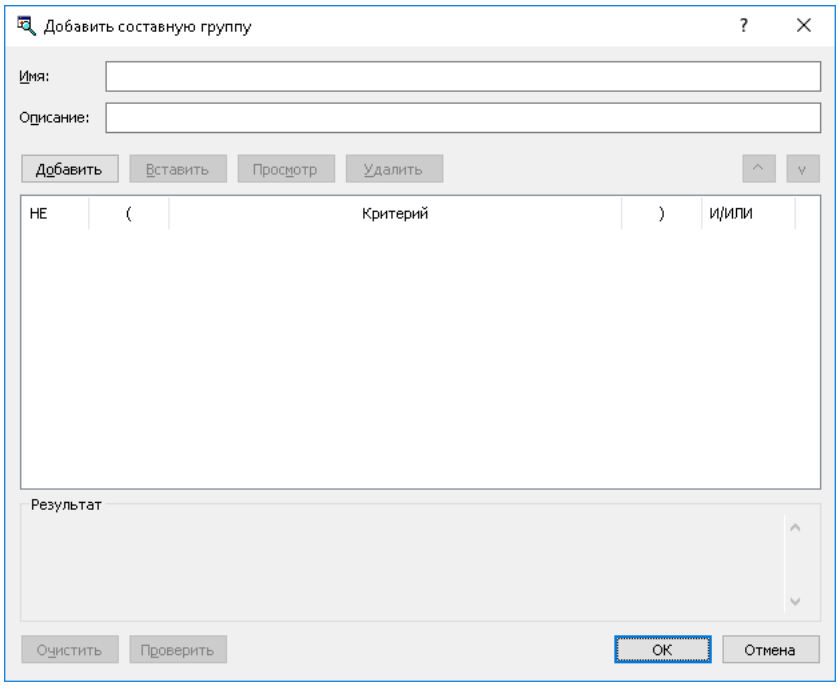
     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

Появится диалоговое окно, подобное приведенному ниже.



4. В верхней части появившегося диалогового окна в области **База данных контента** нажмите стрелку рядом с полем **Добавить группу**, а затем выберите пункт **Составное**.

   Появится диалоговое окно "Добавить составную группу".



5. В диалоговом окне **Добавить составную группу** выполните следующие действия:
   - **Имя** - Указать имя группы.
   - **Описание** - Указать описание группы.
   - **Добавить** - Добавить контентные группы из базы данных контента в конец списка групп в столбце **Критерий**:
     a) Нажмите кнопку **Добавить** или дважды щелкните пустую область в столбце **Критерий**.
     b) В появившемся диалоговом окне выберите контентную группу, а затем нажмите кнопку **OK**, или дважды щелкните контентную группу.

     Чтобы выбрать одновременно несколько контентных групп, используйте клавиши SHIFT или CTRL.

     Чтобы просмотреть контентную группу, выберите группу, а затем нажмите кнопку "Просмотр группы".

     Выбранные контентные группы появятся в столбце "Критерий" диалогового окна "Добавить составную группу". Каждая выбранная контентная группа рассматривается как отдельный критерий фильтра, включенный в логическое выражение.
   - **Вставить** - Добавить контентную группу из базы данных контента перед группой, выбранной в столбце **Критерий**:
     a) Выберите группу в столбце **Критерий**, а затем нажмите кнопку **Вставить**.
     b) В появившемся диалоговом окне выберите контентную группу, а затем нажмите кнопку **OK**, или дважды щелкните контентную группу.
   - **Просмотр** - Просмотреть контентную группу, выбранную в столбце **Критерий**:
     - Выберите группу в столбце **Критерий**, а затем нажмите кнопку **Просмотр**, или дважды щелкните группу для просмотра.
   - **Удалить** - Удалить контентную группу, выбранную в столбце **Критерий**.
   - **НЕ** - Связать выбранную контентную группу логическим оператором NOT. Для этого выберите контентную группу в столбце **Критерий**, а затем установите соответствующий флажок в столбце **НЕ**.
   - **И/ИЛИ** - Связать выбранную контентную группу логическим оператором AND или OR. Для этого выберите контентную группу в столбце **Критерий**, а затем установите соответствующий флажок в столбце **И/ИЛИ**.
   - **Очистить** - Очистить текущий список контентных групп из столбца **Критерий**.
   - **Проверить** - Проверить логическое выражение. Если логическое выражение составлено неправильно (например, число открытых скобок не соответствует числу закрытых), выводится сообщение об ошибке.
6. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Добавить составную группу**.

   Новая контентная группа добавляется в список существующих контентных групп в области "База данных контента" в верхней части диалогового окна для управления контентно-зависимыми правилами.

Примечание: При перемещении какой-либо записи на место соседней в списке групп флажок **НЕ** перемещается вместе с записью, только если количество открывающих скобок меньше или равно количеству закрывающих скобок как в перемещаемой записи, так и в записи, на место которой она перемещается. Если открывающих скобок хотя бы в одной из них больше, чем закрывающих, то этот флажок не переходит на соседнюю запись. Такое решение помогает сохранить логическую структуру выражения при изменении порядка записей в списке.

Просмотр встроенных контентных групп

Встроенные контентные группы можно просматривать, но нельзя изменять или удалять.

Чтобы просмотреть встроенную контентную группу

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства** либо узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно для управления контентно-зависимыми правилами.
4. В верхней части появившегося диалогового окна в области **База данных контента** выберите любую встроенную контентную группу, которую требуется просмотреть, а затем нажмите кнопку **Просмотр группы**.

Дублирование встроенных контентных групп

Встроенные контентные группы невозможно изменять, но можно создавать и использовать их редактируемые копии (дубликаты), необходимые для решения частных задач организации.

Чтобы продублировать встроенную контентную группу

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства** либо узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно для управления контентно-зависимыми правилами.
4. В верхней части появившегося диалогового окна в области **База данных контента** выберите любую встроенную контентную группу, которую требуется продублировать, а затем нажмите кнопку **Дублировать**.
5. В открывшемся диалоговом окне внесите необходимые изменения, а затем нажмите кнопку **OK**.

   Новая контентная группа добавляется в список существующих контентных групп в области "База данных контента" в верхней части диалогового окна для управления контентно-зависимыми правилами.

Редактирование или удаление пользовательских контентных групп

Пользовательские контентные группы можно редактировать или удалять по мере надобности.

Чтобы редактировать или удалить пользовательскую контентную группу

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства** либо узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно для управления контентно-зависимыми правилами.
4. В верхней части появившегося диалогового окна в области **База данных контента** выберите любую пользовательскую контентную группу, которую необходимо изменить или удалить.
5. Нажмите кнопку **Редактировать группу**, чтобы изменить выбранную контентную группу. В открывшемся диалоговом окне внесите необходимые изменения, а затем нажмите кнопку **OK**.

   - или -

   Нажмите кнопку **Удалить группу** или клавишу DELETE, чтобы удалить выбранную контентную группу.
6. В диалоговом окне для редактирование контентно-зависимых правил нажмите кнопку **OK** или **Применить**, чтобы сохранить изменения.

Тестирование контентных групп

Каждую контентную группу можно протестировать, чтобы выяснить, соответствуют ли ей те или иные пробные файлы. Используя эти тесты, можно убедиться, что контентно-зависимые правила, созданные на основе контентных групп, отвечают поставленным бизнес-задачам.

Чтобы протестировать контентную группу

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства** либо узел **Протоколы**.

3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

     - или -

   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

4. В верхней части появившегося диалогового окна в области **База данных контента** выберите любую встроенную контентную группу, которую необходимо протестировать, а затем нажмите кнопку **Тестировать группу**.

   За один раз можно протестировать только одну группу.

5. В открывшемся диалоговом окне найдите и выберите пробный файл, который будет использован для тестирования контентной группы, и нажмите кнопку **Открыть**.

   При тестировании группы цифровых отпечатков необходимо использовать DeviceLock Enterprise Server для проверки отпечатков пробного файла. Поэтому консоль отображает диалоговое окно для указания сервера DeviceLock Enterprise Server, на котором размещена база цифровых отпечатков. Чтобы продолжить тестирование, введите имя компьютера, на котором работает DeviceLock Enterprise Server. Подробнее о методе отпечатков см. в разделе Цифровые отпечатки.

   Консоль сохраняет указанное имя сервера и использует его во время текущего сеанса консоли без повторного запроса. В последующих сеансах консоль вновь отображает диалоговое окно, позволяя выбрать другой сервер. По умолчанию выбирается сервер, использовавшийся в предыдущем сеансе консоли.

После завершения обработки пробного файла появится сообщение о результате теста. Если файл соответствует условиям группы, появится сообщение “Выбранный файл совпадает с группой”. В противном случае появится сообщение “Выбранный файл не совпадает с группой”.

Примечание: Во время тестирования консоль может перестать отвечать (“зависает”).

Управление контентно-зависимыми правилами

Управление контентно-зависимыми правилами предполагает:

- Создание контентно-зависимых правил
- Редактирование контентно-зависимых правил
- Копирование контентно-зависимых правил
- Экспорт и импорт контентно-зависимых правил
- Сброс контентно-зависимых правил в исходное состояние
- Удаление контентно-зависимых правил

Чтобы управлять контентно-зависимыми правилами, можно использовать консоль DeviceLock Management Console, DeviceLock Group Policy Manager или DeviceLock Service Settings Editor.

Создание контентно-зависимых правил

Контентно-зависимые правила создаются на основе встроенных или пользовательских контентных групп. Подробнее об этих группах см. в разделе Настройка контентных групп.

Также можно включить тревожные оповещения о том, что сработало контентно-зависимое правило. Такие оповещения включаются при настройке контентно-зависимого правила.

DeviceLock рассылает тревожные оповещения с учетом настроек, указывающих адресата и способ отправки оповещений. Перед включением оповещений для контентно-зависимых правил задайте параметры оповещений в настройках сервиса DeviceLock (см. раздел Алерты).

В этом разделе рассматривается:

- Создание правил для устройств
- Создание правил для протоколов

Создание правил для устройств

Чтобы создать контентно-зависимое правило для устройств, выполните следующие действия:

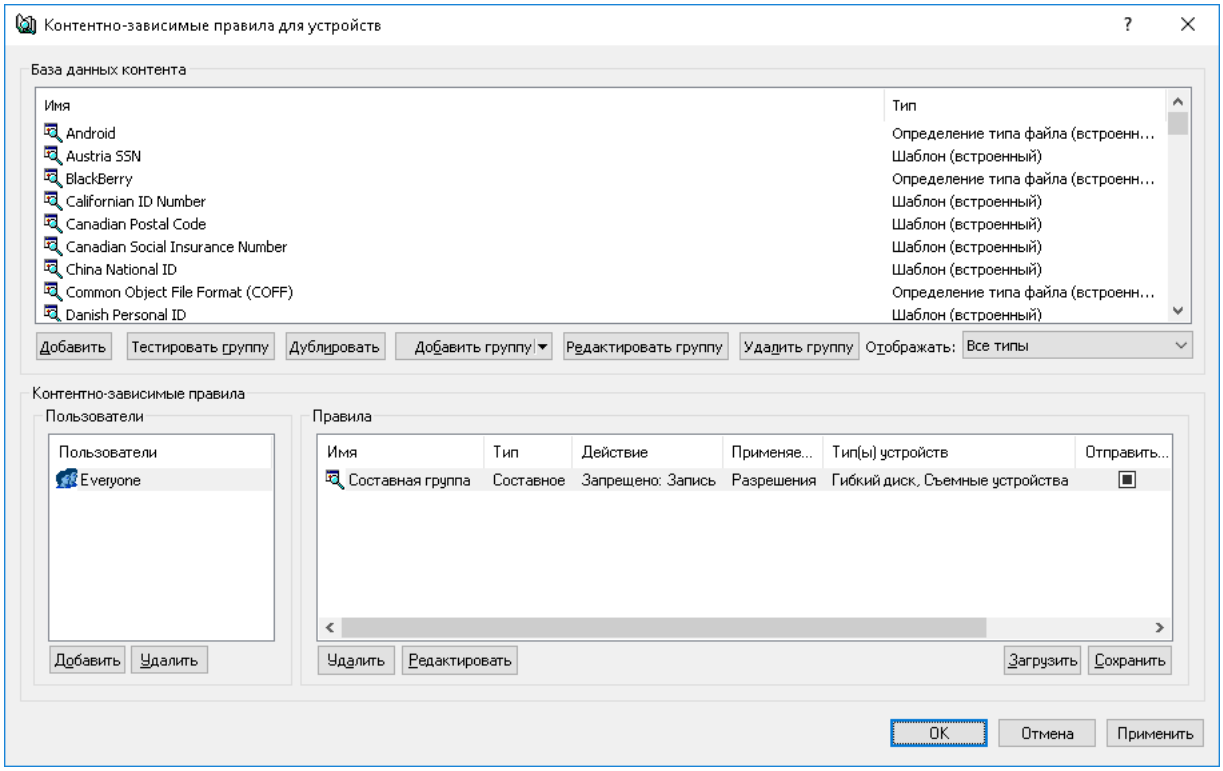
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно, подобное приведенному ниже.



4. В левой нижней части появившегося диалогового окна в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

5. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой нижней части диалогового окна для управления контентно-зависимыми правилами.

   Чтобы удалить пользователя или группу, в области **Пользователи** в левой нижней части диалогового окна для управления правилами выберите пользователя или группу, а затем нажмите кнопку **Удалить** или нажмите клавишу DELETE.

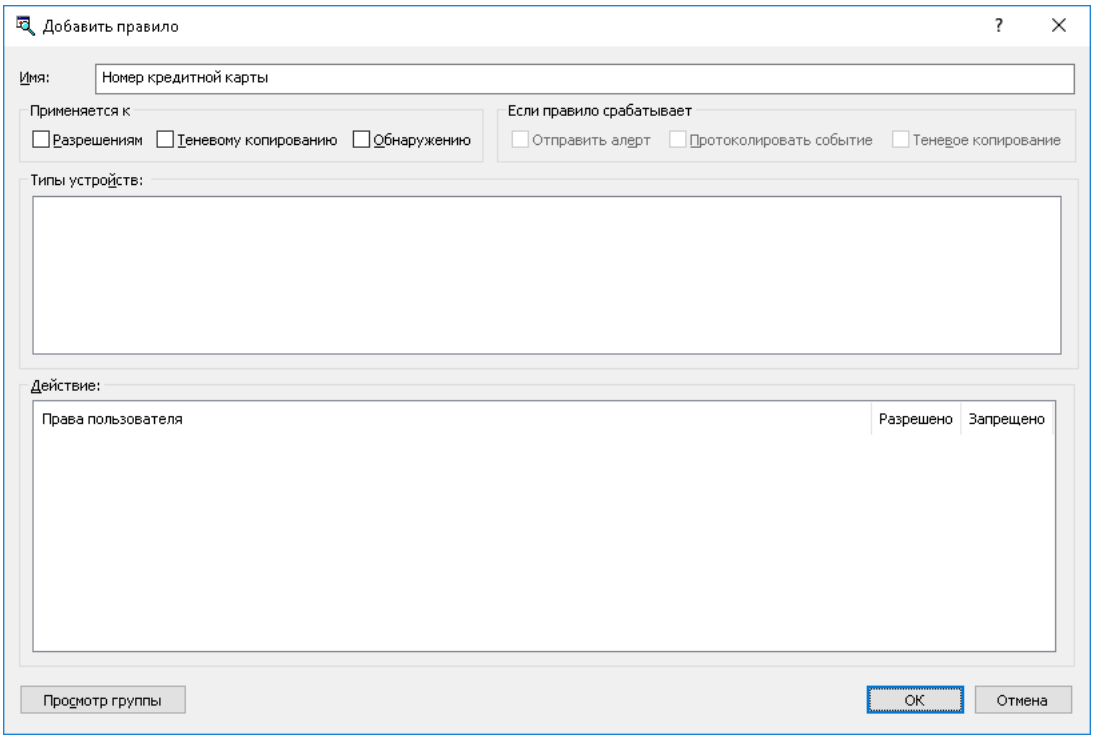
6. В левой нижней части диалогового окна для управления правилами в области **Пользователи** выберите пользователя или группу, для которой требуется задать правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

7. В верхней части диалогового окна для управления правилами в области **База данных контента** выберите необходимую контентную группу, а затем нажмите кнопку **Добавить**, или дважды щелкните необходимую контентную группу.

   Примечание: Для каждого создаваемого контентно-зависимого правила можно указать только одну контентную группу.

   Появится диалоговое окно “Добавить правило”.



8. В диалоговом окне **Добавить правило** в поле **Имя** введите имя контентно-зависимого правила.

   Имя правила по умолчанию совпадает с именем его контентной группы. При необходимости имя правила может быть изменено.

   Для просмотра контентной группы данного правила нажмите кнопку **Просмотр группы** в левом нижнем углу диалогового окна. Консоль отображает свойства группы в отдельном диалоговом окне, позволяя просматривать свойства, но не изменять их.

9. В области **Применяется к** укажите тип операций, к которым должно применяться это правило. Возможные варианты:

   - **Разрешениям** - Указывает, что правило применяется к операциям контроля доступа.
   - **Теневому копированию** - Указывает, что правило применяется к операциям теневого копирования.
   - **Обнаружению** - Указывает, что правило будет обнаруживать указанное содержимое передаваемых данных, при этом будут протоколироваться события обнаружения и отправляться тревожные уведомления, если установлены соответствующие флаги.
   - **Разрешениям**, **Теневому копированию** - Указывает, что правило применяется и к операциям контроля доступа, и к операциям теневого копирования.
   - **Разрешениям, Обнаружению** - Указывает, что правило будет применяться как для операция контроля, так и для операций обнаружения.
   - **Теневому копированию, Обнаружению** - Указывает, что правило будет применяться как для операций избирательного теневого копирования, так и для операций обнаружения.
   - **Разрешениям, Теневому копированию, Обнаружению** - Указывает, что правило будет применяться как для операций контроля и избирательного теневого копирования, так и для операций обнаружения.

   Примечание: Для успешного создания/сохранения правила, применяемого исключительно к операциям обнаружения или же к к операциям обнаружения в совокупности с другими операциями, необходимо установить по крайней мере один из флажков: **Протоколировать событие**, **Отправить алерт** или **Теневое копирование** (см. шаг 10 данной процедуры). В противном случае, правило не сохраняется, и появляется следующее сообщение: “Необходимо выбрать флаг Протоколировать событие, Отправить алерт или Теневое копирование”.

10. В области **Если правило срабатывает** укажите следующие дополнительные операции, которые будут выполняться при срабатывании правила:

    - **Отправить алерт** - Оповещение рассылается при каждом срабатывании правила.
    - **Протоколировать событие** - Событие регистрируется в журнале аудита при каждом срабатывании правила.
    - **Теневое копирование** - Теневая копия данных создается при каждом срабатывании правила.

    При включении или отключении алертов, аудита и/или теневого копирования в контентно-зависимом правиле настройка правила имеет приоритет над соответствующей настройкой для типа устройств.

    Пример: Если аудит включен для некоторого типа устройств и отключен в правиле для этого типа устройств, срабатывание такого правила не вызовет события аудита. Если же аудит в правиле включен, то срабатывание правила вызовет событие аудита, даже если аудит отключен на уровне типа устройств.

Правило может наследовать настройку алертов, аудита и/или теневого копирования, заданную на уровне типа устройств. Эта опция выбрана по умолчанию и представлена неопределенным состоянием флажков (не установленных и не очищенных). Состояние каждого флажка можно изменить независимо от других.

Пример: Если правило наследует настройку аудита, заданную для типа устройств, то срабатывание такого правила вызовет событие аудита только если аудит включен для типа устройств, контролируемых этим правилом.

11. В области **Типы устройств** выберите типы устройств, к которым должно применяться это правило.

    Контентно-зависимые правила могут применяться к следующим типам устройств: Буфер обмена, Гибкий диск, iPhone-устройства, MTP, Оптический привод, Palm, Принтер, Съемные устройства, TC-устройства и Windows Mobile.

    Если выбраны различные типы устройств, имеющие разные наборы возможных прав доступа, в области "Действие" диалогового окна будут показаны все действия, применимые для каждого из выбранных устройств. В результирующем правиле эффективными будут только те действия, которые применимы для конкретного типа устройств.

12. В области **Действие** укажите, какие действия с файлами пользователю разрешены или запрещены, какие действия пользователя будут записываться в журнале теневого копирования, а также при каких событиях будет выполняться проверка с целью обнаружения содержимого.

    Если правило применяется одновременно к операциям контроля доступа и операциям теневого копирования, то опция "Чтение" будет недоступна. Подробнее о правах, которые могут быть заданы в контентно-зависимых правилах, см. в разделах Управление доступом к контенту, Теневое копирование контента и Обнаружение контента для устройств.

13. Нажмите кнопку **OK**.

    Созданное правило отображается в области "Правила" в правой нижней части диалогового окна для управления контентно-зависимыми правилами.

14. Нажмите кнопку **OK** или **Применить**, чтобы применить правило.

Пользователи и группы, для которых заданы контентно-зависимые правила, относящиеся к устройствам, отображаются в дереве консоли под узлом **Устройства** > **Контентно-зависимые правила**. Если в дереве консоли выбрать пользователя или группу, для которой задано правило, на панели сведений отобразится информация о заданном правиле (подробнее см. в разделе Список контентно-зависимых правил для устройств).

Создание правил для протоколов

Чтобы создать контентно-зависимое правило для протоколов, выполните следующие действия:

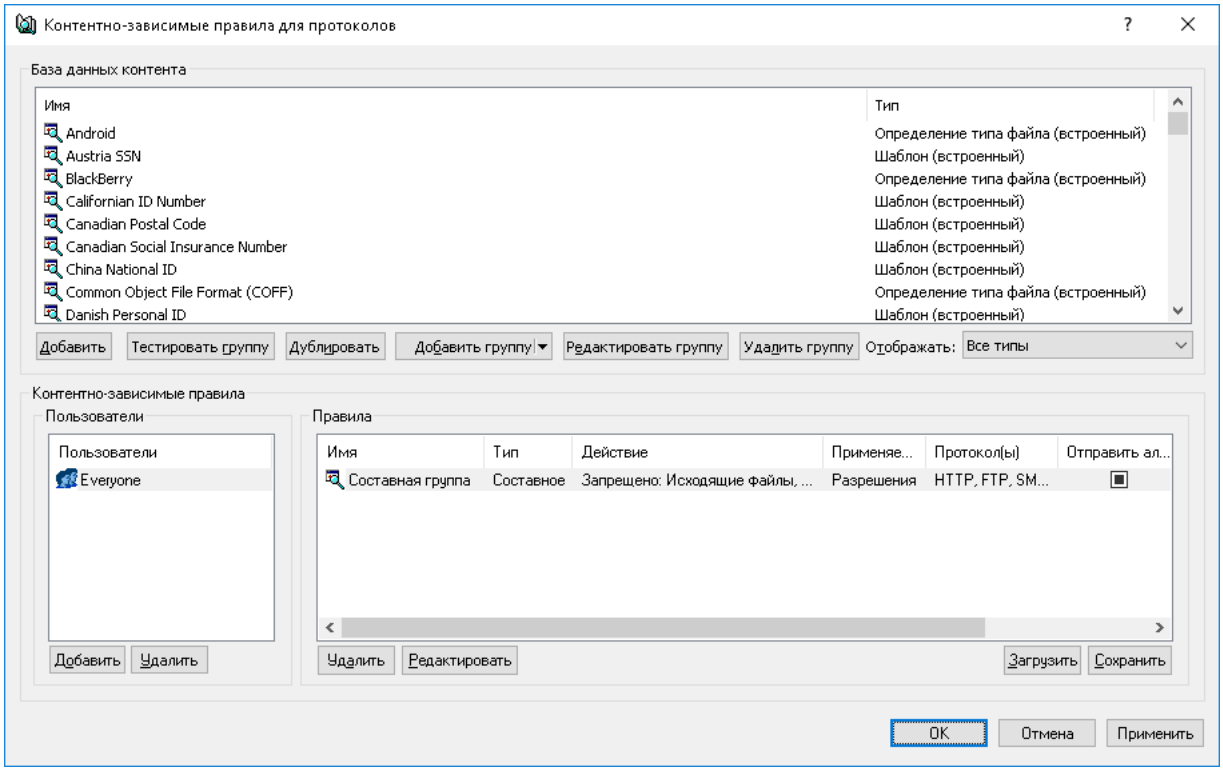
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно, подобное приведенному ниже.



4. В левой нижней части появившегося диалогового окна в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

5. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой нижней части диалогового окна для управления контентно-зависимыми правилами.

   Чтобы удалить пользователя или группу, в области **Пользователи** в левой нижней части диалогового окна для управления правилами выберите пользователя или группу, а затем нажмите кнопку **Удалить** или нажмите клавишу DELETE.

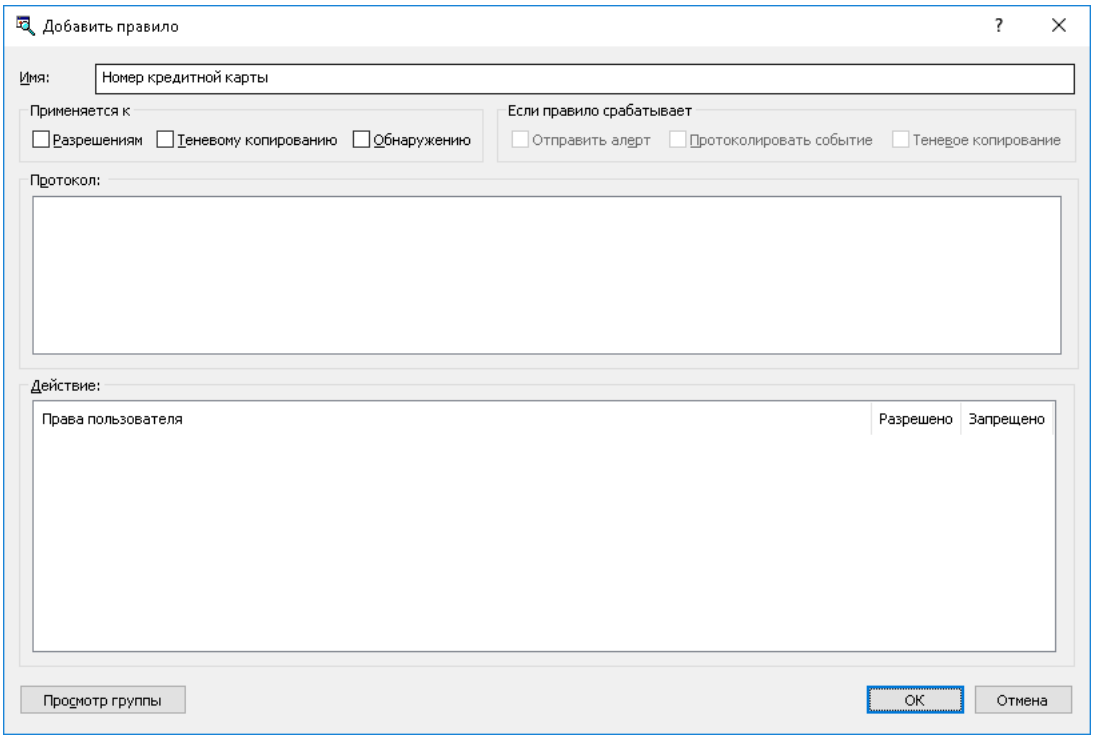
6. В левой нижней части диалогового окна для управления правилами в области **Пользователи** выберите пользователя или группу, для которой требуется задать правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

7. В верхней части диалогового окна для управления правилами в области **База данных контента** выберите необходимую контентную группу, а затем нажмите кнопку **Добавить**, или дважды щелкните необходимую контентную группу.

   Примечание: Для каждого создаваемого контентно-зависимого правила можно указать только одну контентную группу.

   Появится диалоговое окно “Добавить правило”.



8. В диалоговом окне **Добавить правило** в поле **Имя** введите имя контентно-зависимого правила.

   Имя правила по умолчанию совпадает с именем его контентной группы. При необходимости имя правила может быть изменено.

   Для просмотра контентной группы данного правила нажмите кнопку **Просмотр группы** в левом нижнем углу диалогового окна. Консоль отображает свойства группы в отдельном диалоговом окне, позволяя просматривать свойства, но не изменять их.

9. В области **Применяется к** укажите тип операций, к которым должно применяться это правило. Возможные варианты:

   - **Разрешениям** - Указывает, что правило применяется к операциям контроля доступа.
   - **Теневому копированию** - Указывает, что правило применяется к операциям теневого копирования.
   - **Обнаружению** - Указывает, что правило будет обнаруживать указанное содержимое передаваемых данных, при этом будут протоколироваться события обнаружения и отправляться тревожные уведомления, если установлены соответствующие флаги.
   - **Разрешениям**, **Теневому копированию** - Указывает, что правило применяется и к операциям контроля доступа, и к операциям теневого копирования.
   - **Разрешениям, Обнаружению** - Указывает, что правило будет применяться как для операция контроля, так и для операций обнаружения.
   - **Теневому копированию, Обнаружению** - Указывает, что правило будет применяться как для операций избирательного теневого копирования, так и для операций обнаружения.
   - **Разрешениям, Теневому копированию, Обнаружению** - Указывает, что правило будет применяться как для операций контроля и избирательного теневого копирования, так и для операций обнаружения.

   Примечание: Для успешного создания/сохранения правила, применяемого исключительно к операциям обнаружения или же к к операциям обнаружения в совокупности с другими операциями, необходимо установить по крайней мере один из флажков: **Протоколировать событие**, **Отправить алерт** или **Теневое копирование** (см. шаг 10 данной процедуры). В противном случае, правило не сохраняется, и появляется следующее сообщение: “Необходимо выбрать флаг Протоколировать событие, Отправить алерт или Теневое копирование.”

10. В области **Если правило срабатывает** укажите следующие дополнительные операции, которые будут выполняться при срабатывании правила:

    - **Отправить алерт** - Оповещение рассылается при каждом срабатывании правила.
    - **Протоколировать событие** - Событие регистрируется в журнале аудита при каждом срабатывании правила.
    - **Теневое копирование** - Теневая копия данных создается при каждом срабатывании правила.

    При включении или отключении алертов, аудита и/или теневого копирования в контентно-зависимом правиле настройка правила имеет приоритет над соответствующей настройкой для протокола.

    Пример: Если аудит включен для некоторого протокола и отключен в правиле для этого протокола, срабатывание такого правила не вызовет события аудита. Если же аудит в правиле включен, то срабатывание правила вызовет событие аудита, даже если аудит отключен на уровне протокола.

Правило может наследовать настройку алертов, аудита и/или теневого копирования, заданную на уровне протокола. Эта опция выбрана по умолчанию и представлена неопределенным состоянием флажков (не установленных и не очищенных). Состояние каждого флажка можно изменить независимо от других.

Пример: Если правило наследует настройку аудита, заданную для протокола, то срабатывание такого правила вызовет событие аудита только если аудит включен для протокола, контролируемого этим правилом.

11. В области **Протокол** выберите протоколы, к которым должно применяться это правило.

    Контентно-зависимые правила могут применяться к следующим протоколам: Поиск работы, Файловые хранилища, FTP, HTTP, IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMB, SMTP, Социальные сети, Telegram, Viber, Web-почта, Web-поиск, WhatsApp и Zoom.

    Если выбраны различные протоколы, имеющие разные наборы возможных прав доступа, в области "Действие" диалогового окна будут показаны все действия, применимые для каждого из выбранных протоколов. В результирующем правиле эффективными будут только те действия, которые применимы для конкретного протокола.

12. В области **Действие** укажите, какие действия с протоколами пользователю разрешены или запрещены, какие действия пользователя будут протоколироваться в журнале теневого копирования, а также при каких событиях будет выполняться проверка с целью обнаружения содержимого.

    Подробнее о правах, которые могут быть заданы в контентно-зависимых правилах, см. в разделах Управление доступом к контенту, Теневое копирование контента и Обнаружение контента для протоколов.

13. Нажмите кнопку **OK**.

    Созданное правило отображается в области "Правила" в правой нижней части диалогового окна для управления контентно-зависимыми правилами.

14. Нажмите кнопку **OK** или **Применить**, чтобы применить правило.

Пользователи и группы, для которых заданы контентно-зависимые правила, относящиеся к протоколам, отображаются в дереве консоли под узлом **Протоколы** > **Контентно-зависимые правила**. Если в дереве консоли выбрать пользователя или группу, для которой задано правило, на панели сведений отобразится информация о заданном правиле (подробнее см. в разделе Список контентно-зависимых правил для протоколов).

Редактирование контентно-зависимых правил

Можно редактировать свойства заданных контентно-зависимых правил, такие как **Имя**, **Применяется к**, **Если правило срабатывает, Протокол, Действие**.

Чтобы редактировать контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Выполните одно из следующих действий:
   - В случае правила для устройств раскройте узел **Устройства**.
   - В случае правила для протоколов раскройте узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** щелкните правой кнопкой мыши **Контентно-зависимые правила**, выберите команду **Управление**, а затем выполните следующее:
   a) В левой нижней части появившегося диалогового окна в области **Пользователи** выберите пользователя или группу, правило для которой требуется редактировать.

      Если выбрать пользователей или группы, в области "Правила" в правой нижней части диалогового окна отображаются контентно-зависимые правила, которые применяются к этим пользователям или группам.
   b) В правой нижней части диалогового окна в области **Правила** выберите правило, которое требуется редактировать, а затем нажмите кнопку **Редактировать**.

      - или -

      Щелкните правой кнопкой мыши правило, а затем выберите команду **Редактировать**.

      - или -

      Дважды щелкните правило.

   - или -

   В узле **Устройства** или в узле **Протоколы** раскройте узел **Контентно-зависимые правила**, а затем выполните следующее:
   a) В узле **Контентно-зависимые правила** выберите пользователя или группу, правило для которой требуется редактировать.

      Если выбрать пользователей или группы, на панели сведений отображаются контентно-зависимые правила, которые применяются к этим пользователям или группам.

b) На панели сведений щелкните правой кнопкой мыши правило, которое требуется редактировать, а затем выберите команду **Редактировать**.

   - или -

   На панели сведений дважды щелкните правило, которое требуется редактировать.

Появится диалоговое окно "Редактирование правила".

4. В диалоговом окне **Редактирование правила** внесите необходимые изменения.
5. Нажмите кнопку **OK**, чтобы применить изменения.

Копирование контентно-зависимых правил

Можно выполнять операции вырезать-вставить, копировать-вставить, а также операции перетаскивания, чтобы повторно использовать существующие контентно-зависимые правила.

Чтобы скопировать контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Выполните одно из следующих действий:
   - В случае правила для устройств раскройте узел **Устройства**.
   - В случае правила для протоколов раскройте узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно для управления контентно-зависимыми правилами.
4. В левой нижней части диалогового окна для управления правилами в области **Пользователи** выберите пользователя или группу, правило для которой требуется скопировать.

   Если выбрать пользователей или группы, в области "Правила" в правой нижней части диалогового окна отображаются контентно-зависимые правила, которые применяются к этим пользователям или группам.

5. В правой нижней части диалогового окна для управления правилами в области **Правила** щелкните правой кнопкой мыши правило, которое требуется скопировать, а затем выберите команду **Копировать** или **Вырезать**.

   Вырезанное или скопированное правило автоматически копируется в буфер обмена.

   Также можно использовать сочетания клавиш CTRL+C, CTRL+X и CTRL+V, чтобы скопировать, вырезать и вставить правило. При нажатии CTRL+X правило будет вырезано только после того, как вы его вставите.

   Для выполнения операции перетаскивания выделите правило и перетащите его к пользователю или группе, к которой требуется применить скопированное правило.

6. В левой нижней части диалогового окна для управления правилами в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно "Выбор: "Пользователи" или "Группы"".

7. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых должно применяться скопированное правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области "Пользователи" в левой нижней части диалогового окна для управления контентно-зависимыми правилами.

8. В левой нижней части диалогового окна для управления правилами в области **Пользователи** выберите пользователей или группы, к которым требуется применить скопированное правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

9. В правой нижней части диалогового окна для управления правилами щелкните правой кнопкой мыши в области **Правила**, а затем выберите команду **Вставить**.

   Скопированное правило отображается в области "Правила" в правой нижней части диалогового окна для управления контентно-зависимыми правилами.

10. Нажмите кнопку **OK** или **Применить**, чтобы применить скопированное правило.

Экспорт и импорт контентно-зависимых правил

Можно экспортировать все заданные контентно-зависимые правила в файл с расширением .cwl, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт правил также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать контентно-зависимые правила

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Выполните одно из следующих действий:

   - В случае правил для устройств раскройте узел **Устройства**.
   - В случае правил для протоколов раскройте узел **Протоколы**.

3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Сохранить**.

     - или -

   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Сохранить** на панели инструментов.

     - или -

   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши любого пользователя или группу, для которой задано правило, а затем выберите команду **Сохранить**.

     - или -

   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой правило, а затем выберите команду **Сохранить**.

     - или -

   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило, а затем щелкните значок **Сохранить** на панели инструментов.

     - или -

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**. В правой нижней части появившегося диалогового окна для в области **Правила** нажмите кнопку **Сохранить**.

4. В появившемся диалоговом окне выберите папку, в которую требуется сохранить файл, задайте имя файла, и нажмите кнопку **Сохранить**.

   При экспорте правила сохраняются в файле с расширением .cwl.

Чтобы импортировать контентно-зависимые правила

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Выполните одно из следующих действий:

   - В случае правил для устройств раскройте узел **Устройства**.
   - В случае правил для протоколов раскройте узел **Протоколы**.

3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Загрузить**.

     - или -

   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Загрузить** на панели инструментов.

     - или -

   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши любого пользователя или группу, для которой задано правило, а затем выберите команду **Загрузить**.

     - или -

   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, а затем выберите команду **Загрузить**.

     - или -

   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило, а затем щелкните значок **Загрузить** на панели инструментов.

     - или -

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**. В правой нижней части появившегося диалогового окна в области **Правила** нажмите кнопку **Загрузить**.

4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

   За один раз можно импортировать только один файл .cwl.

Сброс контентно-зависимых правил в исходное состояние

Если для развертывания политик DeviceLock используется DeviceLock Group Policy Manager или DeviceLock Service Settings Editor, могут возникнуть ситуации, когда потребуется отменить применение заданных контентно-зависимых правил к определенной группе компьютеров. Для этого необходимо вернуть ранее заданные контентно-зависимые правила в исходное "неопределенное" состояние. Все параметры DeviceLock, которые установлены в состояние "не определен", игнорируются на клиентских компьютерах.

Чтобы сбросить контентно-зависимые правила в исходное "неопределенное" состояние

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.
   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Выполните одно из следующих действий:
   - В случае правил для устройств раскройте узел **Устройства**.
   - В случае правил для протоколов раскройте узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Сбросить**.

Удаление контентно-зависимых правил

Можно удалять контентно-зависимые правила, если они больше не нужны.

Чтобы удалить контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Выполните одно из следующих действий:
   - В случае правила для устройств раскройте узел **Устройства**.
   - В случае правила для протоколов раскройте узел **Протоколы**.
3. В узле **Устройства** или в узле **Протоколы** выполните одно из следующих действий:
   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши пользователя или группу, для которой задано правило, а затем выберите команду **Удалить пользователя**.

     Если удалить пользователя или группу, все правила, заданные для этого пользователя или группы, автоматически удалятся.

     - или -
   - Раскройте **Контентно-зависимые правила**, затем выберите пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, заданное для этого пользователя или группы, а затем выберите команду **Удалить**.

     - или -
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**. В левой нижней части появившегося диалогового окна в области **Пользователи** выберите пользователя или группу, для которой задано правило. В правой нижней части этого диалогового окна в области **Правила** выберите правило и затем нажмите кнопку **Удалить** или щелкните правой кнопкой мыши правило и затем выберите команду **Удалить**.

     Чтобы выбрать одновременно несколько правил, используйте клавиши SHIFT или CTRL.

6

Цифровые отпечатки

В этой главе:

О методе цифровых отпечатков

Управление цифровыми отпечатками

Применение цифровых отпечатков

О методе цифровых отпечатков

Цифровые отпечатки - это один из методов, которые используются программным комплексом DeviceLock для идентификации данных, передаваемых через различные устройства и сетевые протоколы. В его основе лежит сопоставление документов или файлов с так называемыми цифровыми отпечатками - наборами буквенно-цифровых строк (хэшей), при помощи которых можно идентифицировать данные, хранящиеся в документе или файле.

При использовании этого метода DeviceLock снимает цифровые отпечатки с образцов конфиденциальных документов, а затем сравнивает их с цифровыми отпечатками проверяемых документов. Если процент "соответствия отпечатков" превышает требуемый порог в соответствии с настройкой, проверяемые документы считаются конфиденциальными, и к ним применяются все необходимые действия по обеспечению безопасности.

Использование цифровых отпечатков позволяет обеспечить идентификацию и защиту информации, находящейся в файлах или передаваемой по сети. Например, их можно использовать для идентификации финансовых данных, хранящихся в документах MS Office, бизнес-информации, хранящейся в файлах PDF, или исходного кода, хранящегося в текстовых файлах. Кроме того, цифровые отпечатки можно использовать для идентификации и защиты нетекстовых файлов (таких как изображения, чертежи и мультимедийные файлы) а также для идентификации бинарных данных при их копировании из одного файла в другой.

С помощью цифровых отпечатков можно обнаруживать как полностью скопированные документы, так и отдельные фрагменты документов, даже если в документ были внесены изменения. Цифровые отпечатки позволяют надежно опознавать содержимое документа, несмотря на его возможное искажение, вызванное добавлением несущественной информации (отдельных букв или символов, малозначимых слов и т.п.).

Цифровые отпечатки особенно эффективны при идентификации стандартных документов, которые изменяются незначительно. Например, они позволяют легко идентифицировать заполненные контракты, отличающиеся только данными одной из сторон. Благодаря надежной идентификации данных, хранящихся в документах и файлах, цифровые отпечатки помогают отслеживать и защищать конфиденциальную информацию, обеспечивая масштабируемое применение средств ее защиты при передаче через корпоративную сеть и/или на периферийные пользовательские устройства.

Как этот метод устроен

Метод цифровых отпечатков основан на взаимодействии следующих элементов:

- Контентно-зависимые правила
- Контентные группы
- Классификации цифровых отпечатков
- Цифровые отпечатки документов и файлов
- База данных цифровых отпечатков
- Процент соответствия
- Нормализация отпечатков

Контентно-зависимые правила

Контентно-зависимые правила могут использовать контентные группы цифровых отпечатков для анализа данных на основе цифровых отпечатков. Такие правила могут применяться как к устройствам, так и к сетевым протоколам, позволяя использовать цифровые отпечатки для управления разрешениями на доступ/передачу контента, контентно-зависимым созданием теневых копий и/или простым обнаружением контента.

Контентные группы

Контентные группы цифровых отпечатков реализуют проверку контента с использованием цифровых отпечатков. Каждая такая группа ссылается на определенную классификацию отпечатков и позволяет задать минимальный процент соответствия отпечатков (называемый порогом), который требуется для присвоения данной классификации проверяемому контенту.

Классификации цифровых отпечатков

Конфиденциальные документы и другие информационные активы, требующие защиты, могут быть распределены по классификациям с определенными уровнями важности или секретности (например, “Для служебного пользования”, “Конфиденциально”, “Секретно” и “Совершенно секретно”). Их цифровые отпечатки классифицируются аналогично, так что классификация каждого уровня содержит отпечатки информации соответствующего уровня важности. Каждая классификация представляет собой контейнер, в котором хранятся цифровые отпечатки образцов информации, отнесенной к определенному уровню важности или секретности. Классификации упорядочиваются в соответствии с этим уровнем.

DeviceLock предоставляет ряд встроенных классификаций и позволяет добавлять дополнительные пользовательские классификации. При необходимости их порядок по степени важности можно изменить; однако уровень встроенной классификации “Открытая информация” всегда ниже уровня любой другой классификации и не может быть поднят. Цифровые отпечатки из классификации “Открытая информация” имеют минимально возможный уровень независимо от того, встречаются ли они в других классификациях или нет.

Цифровые отпечатки документов и файлов

Набор хэшей, однозначно идентифицирующих документ или файл и его содержимое, называется цифровым отпечатком этого документа или файла. Отпечатки образцов документов и файлов, классификация которых известна, могут быть сохранены в базе данных, где им присваивается та же классификация. Затем проверяемые документы и файлы можно классифицировать путем сравнения их отпечатков с отпечатками из базы данных. Таким образом, накопление и хранение отпечатков играет ключевую роль в последующей классификации документов и файлов.

База данных цифровых отпечатков

Сервер DeviceLock Enterprise Server хранит цифровые отпечатки предоставленных ему образцов информации (таких как документы и файлы) в базе данных отпечатков, и позволяет управлять отпечатками, хранящимися в этой базе данных. Отпечатки группируются согласно классификации их источника. Например, отпечатки образцов "секретных" документов попадают в классификацию "Секретно".

База данных обслуживается задачами, выполняемыми на сервере. Для каждой классификации можно создать задачи, которые обрабатывают определенные источники информации (например, наборы документов), специально подобранные для данной классификации. Например, задача для классификации "Конфиденциально" может быть настроена на обработку папки с образцами "конфиденциальных" файлов. Отпечатки, созданные такой задачей, относятся к классификации "Конфиденциально" и могут быть использованы для идентификации других документов или файлов как "конфиденциальных" путем сопоставления отпечатков этих документов или файлов с отпечатками образцов "конфиденциальных" файлов.

Процент соответствия

При проверке источника информации (например, документа или файла) DeviceLock может сравнивать цифровые отпечатки источника с отпечатками определенной классификации из базы данных и вычислять их процент соответствия. Если процент соответствия превышает установленный порог, DeviceLock соответствующим образом классифицирует проверенную информацию. Для "секретных" документов порог соответствия может быть относительно низким, так как даже небольшие фрагменты таких документов могут содержать очень важную информацию. И наоборот, для того, чтобы документ был признан "несекретным", большое количество его фрагментов должно соответствовать образцам "несекретных" документов, поэтому порог соответствия должен быть относительно высоким. Значение порога соответствия выбирается при настройке контентной группы отпечатков документов для контентно-зависимых правил.

Процент соответствия вычисляется как большее из двух значений:

- Процент элементов отпечатков источника, которые соответствуют отпечаткам из определенной классификации в базе данных
- Общий процент элементов отпечатков из определенной классификации в базе данных, которые соответствуют отпечатку источника

Первое значение отвечает ситуации, когда источник содержит фрагменты различных образцов конфиденциальных информации; второе значение позволяет правильно классифицировать источник, содержащий образцы конфиденциальной информации наряду с большим количеством открытой информации. Вместе эти два значения позволяют корректно обрабатывать большинство случаев идентификации контента на основе цифровых отпечатков.

Нормализация отпечатков

Чтобы оптимизировать и ускорить процесс сопоставления отпечатков, отпечатки в базе данных подвергаются нормализации: элементы отпечатков, попавших в классификацию "Открытая информация", удаляются из всех отпечатков, хранящихся в других классификациях. Предполагается, что такие документы заведомо не содержат конфиденциальной информации. Если документ попал в классификацию "Открытая информация", то содержащаяся в нем информация не будет идентифицирована как "секретная" или "конфиденциальная", даже если ее отпечатки имеются в других классификациях.

Сбор и хранение отпечатков

Образцы информационных ресурсов (документы, файлы и т.п.), отпечатки которых собраны и сохранены в базе данных, называются источниками отпечатков. Эти образцы могут быть изменены, добавлены или удалены, или уровень их секретности может со временем меняться. Для того, чтобы база данных учитывала все такие изменения, сервер регулярно выполняет задачи классификации, что приводит к обновлению хранилища отпечатков, как описано ниже.

Обработка образцов информации и снятие их отпечатков осуществляется задачами на сервере DeviceLock Enterprise Server. Каждая такая задача относится к определенной классификации и присваивает ее тем отпечаткам, которые она создает. Например, отпечатки, созданные задачей классификации “Конфиденциально”, относятся к той же классификации “Конфиденциально”.

При каждом запуске задача может проверять файлы в определенной папке. Для каждого файла она сначала создает его отпечатки и сравнивает их с отпечатками из базы данных. Дальнейшая обработка отпечатков файла зависит от результатов сравнения, как указано в следующих примерах:

- В классификации уже содержится отпечаток, источник которого имеет ту же контрольную сумму, путь и имя, что и проверяемый файл. В этом случае задача не вносит изменений в хранилище отпечатков. Однако в случае другого пути или имени файл указывается как еще один источник этого отпечатка в базе данных.
- Контрольная сумма файла отличается от контрольной суммы источника существующего отпечатка, но отпечаток файла в некоторой степени соответствует существующему отпечатку. В этом случае результат выполнения задачи зависит от процента совпадающих элементов этих отпечатков.

  Если процент совпадающих элементов не превышает установленного порога, отпечаток файла добавляется в базу данных как новый отпечаток, у которого этот файл указан в качестве источника.

  Если процент совпадающих элементов превышает установленный порог, то отпечаток файла указывается как новая версия отпечатка, уже существующего в базе данных. В этом случае файл указывается как еще один источник этого отпечатка, если его путь или имя отличается от пути и/или имени других источников.
- Отпечаток файла не соответствует ни одному отпечатку из базы данных. В этом случае отпечаток файла добавляется в базу данных как новый отпечаток, у которого этот файл указан в качестве источника.

Даже если источник отпечатка удален, отпечаток остается в базе данных. Администраторы DeviceLock могут вручную удалять отпечатки или их отдельные версии с помощью консоли DeviceLock Management Console.

Порог создания версий отпечатков

Порог создания версий определяет создавать ли новый отпечаток или просто добавить новую версию к уже существующему. На сервере DeviceLock Enterprise Server указываются отдельные пороговые значения для текстового контента (например, текстовых файлов) и для двоичного контента (например, файлов изображений).

Многие файлы содержат контент обоих типов. Например, документы Microsoft Word представляют собой двоичные файлы, которые могут содержать текст и изображения. Отпечатки файлов со смешанным контентом содержат элементы, идентифицирующие текстовый контент и элементы, идентифицирующие двоичный контент. При классификации такого "смешанного" отпечатка сервер применяет оба пороговых значения, отдельно оценивая процент соответствия для "текстовых" и "двоичных" элементов отпечатка. Это приводит к следующим эффектам:

- Отпечаток текстового файла может быть классифицирован как версия отпечатка для файла со смешанным контентом, и наоборот, "смешанный" отпечаток может оказаться версией отпечатка текстового файла.
- Отпечаток двоичного файла, который не содержит текста, может быть классифицирован как версия отпечатка для файла со смешанным контентом, и наоборот, "смешанный" отпечаток может оказаться версией отпечатка двоичного файла без текстового контента.

Сравнение отпечатков

Чтобы проверить информацию (например, файлы, документы или сообщения) путем ее сопоставления с базой данных отпечатков, DeviceLock использует контентно-зависимые правила, основанные на контентных группах цифровых отпечатков. Группа определяет классификацию применяемых отпечатков и указывает, требуется ли точное совпадение или частичное совпадение. В случае частичного совпадения группа определяет порог соответствия в процентах.

Поскольку база данных отпечатков размещается на сервере DeviceLock Enterprise Server, а контентно-зависимые правила обрабатываются локально на клиентских компьютерах, сервис DeviceLock запрашивает сервер для оценки отпечатков проверяемой информации. По этой причине в настройках сервиса DeviceLock требуется указать хотя бы один экземпляр сервера. Для повышения отказоустойчивости и/или производительности на крупных площадках могут быть указаны несколько работающих экземпляров сервера.

Если серверная база данных отпечатков недоступна

Если сервер DeviceLock Enterprise Server недоступен или недоступна его база данных отпечатков, то сервис DeviceLock на локальном клиентском компьютере не может применять правила, основанные на цифровых отпечатках, а также составные правила, в состав которых входит проверка отпечатков. При этом сервис блокирует попытки передачи информации, которая должна быть проверена такими правилами. Например, если правило контролирует передачу конфиденциальной информации путем проверки ее отпечатков, но сервер базы данных отпечатков недоступен, то сервис DeviceLock не допустит передачу информации, которая должна быть проверена этим правилом.

Проверка отпечатков внутри архива

Предположим, что у сервиса DeviceLock включен параметр Проверка содержимого архивов при чтении и/или Проверка содержимого архивов при записи. В этом случае, применяя контентно-зависимые правила к файлам-архивам, сервис DeviceLock применяет их к каждому файлу, содержащемуся в архиве (см. описание функции Проверка файлов внутри архивов). Однако он может не выполнять проверку отпечатков файлов, находящихся внутри архива, при обнаружении полного совпадения файла-архива с файлом-источником отпечатка из базы данных.

Рассмотрим следующий сценарий:

- У сервиса DeviceLock включен параметр Проверка содержимого архивов при чтении и/или Проверка содержимого архивов при записи.
- У контентной группы цифровых отпечатков включен параметр **Точное совпадение файла** (см. Диалоговое окно для настройки группы цифровых отпечатков).
- Правило, использующее эту группу при проверке некоторого файла-архива, обнаруживает, что контрольная сумма этого файла-архива совпадает с контрольной суммой какого-либо файла-источника отпечатка из базы данных.

В таком случае правило применяется к файлу-архиву без проверки отпечатков файлов, находящихся внутри архива. Весь архив будет разрешен либо запрещен в соответствии с настройками правила.

Тем не менее, при отсутствии совпадения контрольной суммы файла-архива с контрольными суммами файлов-источников отпечатков, правило будет применено к каждому файлу внутри архива. В случае разрешающего правила архив будет разрешен, если правило разрешит каждый из этих файлов; в случае запрещающего правила весь архив будет запрещен, если правило запретит хотя бы один из файлов, содержащихся в данном архиве.

Приступая к работе с цифровыми отпечатками

Чтобы использовать цифровые отпечатки, администратор DeviceLock вначале собирает образцы документов и файлов, которые требуется защитить, и классифицирует их на сервере DeviceLock Enterprise Server с помощью задач классификации, снимающих отпечатки каждого такого файла и его содержимого. Подробнее см. в разделе Задачи отпечатков. Файлы для снятия отпечатков могут размещаться в локальной папке сервера или в общей сетевой папке. Нет необходимости копировать файлы на компьютер, на котором работает сервер DeviceLock Enterprise Server, однако сервер должен иметь достаточные права для доступа и чтения этих файлов там, где они размещены.

Далее администратор DeviceLock должен создать контентные группы, ссылающиеся на классификации цифровых отпечатков, и настроить контентно-зависимые правила на основе этих контентных групп. Подробнее см. в разделе Группы цифровых отпечатков. Поскольку база данных отпечатков находится на сервере, а контентно-зависимые правила обрабатываются на клиентских компьютерах, необходимо указать хотя бы один сервер DeviceLock Enterprise Server в настройках сервиса DeviceLock. Подробнее см. в разделе Настройки сервиса для цифровых отпечатков. В результате сервис DeviceLock сможет использовать правила для проверки информации путем сопоставления ее отпечатков с отпечатками, хранящимися в базе данных.

К примеру, предположим, что образцы секретных документов и файлов - это несколько документов MS Office Word, Excel и PowerPoint, а также несколько файлов изображений (например, PNG или JPEG). Вначале администратор DeviceLock создает и запускаете задачу классификации “Конфиденциально”, которая указывает на папку, содержащую эти документы и файлы. В результате их отпечатки будут созданы и сохранены в базе данных сервера DeviceLock Enterprise Server. Затем администратор создает контентную группу цифровых отпечатков, выбрав для нее уровень классификации “Конфиденциально”. При настройке группы можно установить порог соответствия, т.е. минимальный процент соответствия отпечатков, который требуется для присвоения данного уровня классификации проверяемому контенту. Предположим, что этот порог установлен в 50%. Наконец, администратор создает контенто-зависимое правило на основе созданной группе цифровых отпечатков. Это правило может быть настроено, например, для управления доступом, теневым копированием и/или обнаружением контента.

При применении этого правила к файлу сервис DeviceLock проверяет файл, а также текстовое содержимое файла, если его удается извлечь, путем сопоставления их отпечатков с отпечатками из классификации “Конфиденциально”, хранящимися в базе данных. В данном примере, если процент соответствия отпечатков составляет 50% или более, правило вступает в силу, в результате чего сервис DeviceLock выполняет действия, заданные в настройках этого правила для модуля ContentLock или Discovery (это может быть, например, запрет, разрешение, теневое копирование, тревожное оповещение, обнаружение и обработка контента, и т.д.).

Управление цифровыми отпечатками

Сервер DeviceLock Enterprise Server сохраняет цифровые отпечатки предоставленных ему образцов информации (например, документов и файлов) и позволяет управлять созданием, классификацией и хранением отпечатков:

- Настройки отпечатков - Просмотреть или изменить настройки управления отпечатками, например, порог создания версий отпечатков.
- Задачи отпечатков - Настроить, запустить или проверить задачи, снимающие и классифицирующие отпечатки образцов информации. Если нужно, создать и настроить дополнительные классификации.
- База отпечатков - Просмотреть сведения о сохраненных отпечатках, их версиях и источниках. При необходимости добавить или удалить отпечатки, или удалить их отдельные версии.
- Журнал отпечатков - Просмотреть события, связанные с управлением и обработкой отпечатков на сервере DeviceLock Enterprise Server.

Настройки отпечатков

Порог создания версий отпечатков входит в число настроек управления отпечатками. Он определяет условия, при которых сервер создает новые отпечатки вместо добавления новых версий к отпечаткам, уже имеющимся в базе данных (см. Сбор и хранение отпечатков).

Эти настройки доступны на панели сведений, если в дереве консоли выбрать **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **Настройки отпечатков**.

Предусмотрены следующие настройки:

- Порог версионности для текста - Определяет, следует ли считать данный отпечаток образца текстового контента новым отпечатком или версией существующего.
- Порог версионности для бинарных данных - Определяет, следует ли считать данный отпечаток образца двоичного контента новым отпечатком или версией существующего.

При классификации отпечатков смешанного контента (например, документов Microsoft Word), сервер применяет оба пороговых значения, отдельно оценивая процент соответствия для “текстовых” и “двоичных” элементов отпечатка. Подробнее см. в разделе Порог создания версий отпечатков.

Порог версионности для текста

Эта настройка применяется к текстовому контенту (например, к текстовым файлам) и определяет минимальный процент совпадающих элементов отпечатка, который позволяет считать отпечаток данного контента версией существующего отпечатка. Если процент совпадающих элементов ниже этого порога, сервер добавляет новый отпечаток в базу данных; в противном случае он добавляет новую версию существующего отпечатка.

Чтобы задать желаемое процентное значение, дважды щелкните эту настройку на панели сведений и используйте появившееся диалоговое окно.

См. также:

Сбор и хранение отпечатков

Порог версионности для бинарных данных

Эта настройка применяется к двоичному контенту (например, к файлам изображений) и определяет минимальный процент совпадающих элементов отпечатка, который позволяет считать отпечаток данного контента версией существующего отпечатка. Если процент совпадающих элементов ниже этого порога, сервер добавляет новый отпечаток в базу данных; в противном случае он добавляет новую версию существующего отпечатка.

Чтобы задать желаемое процентное значение, дважды щелкните эту настройку на панели сведений и используйте появившееся диалоговое окно.

См. также:

Сбор и хранение отпечатков

Задачи отпечатков

Образцы информационных ресурсов, требующих защиты (документы, файлы и т.д.), обрабатываются задачами с целью создания и сохранения их отпечатков на сервере. Каждая такая задача относится к определенной классификации и присваивает ее тем отпечаткам, которые она создает. Например, отпечатки, созданные задачей классификации “Конфиденциально”, относятся к той же классификации “Конфиденциально”.

Классификации перечислены в дереве консоли под узлом **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **Задачи отпечатков**. Для просмотра задач, относящихся к определенной классификации, выберите эту классификацию под узлом **Задачи отпечатков** в дереве консоли.

Контекстное меню узла **Задачи отпечатков** предоставляет следующую команду:

- **Редактировать классификации** - Позволяет создавать, переименовывать и удалять пользовательские классификации. Можно также повышать или понижать их уровни. Подробнее см. в разделе Управление классификациями.

Если в дереве консоли выбран узел **Задачи отпечатков**, на панели сведений отображаются имена классификаций, доступных в данный момент на сервере. Контекстное меню каждой классификаций предоставляет следующие команды:

- **Создать задачу** - Создать и настроить новую задачу для выбранной классификации (см. Создание задач).
- **Обновить** - Обновить список на панели сведений с учетом последних изменений.

  Эти команды имеются также в контекстном меню каждой классификации под узлом **Задачи отпечатков** в дереве консоли (см. Управление существующими задачами).

Управление задачами предполагает:

- Создание задач
- Управление существующими задачами
- Просмотр отчетов о выполнении задач

Создание задач

Для создания задачи требуется выполнить следующие действия:

1. Выбрать классификацию, для которой требуется создать задачу.

   Каждая задача относится к определенной классификации и присваивает ее отпечаткам, которые она создает. Например, отпечатки, созданные задачей классификации “Конфиденциально”, относятся к той же классификации “Конфиденциально”.

2. Выполнить команду **Создать задачу** для требуемой классификации в разделе **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **Задачи отпечатков**.

   Эту команду можно выбрать из контекстного меню данной классификации в дереве консоли или на панели сведений, а также из контекстного меню какой-либо задачи, уже имеющейся в данной классификации.

3. Настроить параметры задачи в появившемся диалоговом окне (см. Диалоговое окно для настройки задачи).

Диалоговое окно для настройки задачи

В диалоговом окне для настройки задачи можно просмотреть или изменить следующие параметры:

- **Имя задачи** - Имя, позволяющее идентифицировать задачу.
- **Классификация** - Имя классификации отпечатков, которые создаются данной задачей. Этому параметру присваивается имя классификации, выбранной при создании задачи.
- **Активно** - Установите этот флажок, чтобы включить автоматическое выполнение задачи сервером. Когда этот флажок снят, задачу можно запускать только вручную при помощи консоли.
- **Расписание** - Следующие параметры указывают, когда сервер должен запускать данную задачу:
  - **Обновлять автоматически при изменении содержимого директории** - Сервер запускает задачу, когда обнаруживает изменения в любой из папок, подлежащих обработке этой задачей.

    Примечание: Сервер может задержать запуск задачи примерно на полминуты после обнаружения изменений.

  - **Обновлять каждые** <число> **минут** - Сервер запускает задачу каждый раз по истечении указанного количества минут. Можно задать желаемое количество минут.

  Если флажок **Активно** снят, параметры **Расписание** не действуют.
- **Параметры** - Следующие параметры определяют документы и файлы, которые будут обрабатываться данной задачей:
  - **Искать** - Имена файлов для обработки. Для разделения имен используйте точку с запятой (;). Чтобы обозначить любую группу символов внутри имени, используйте звездочку (*). Пустое поле означает поиск и обработку любых файлов.

    Например, `*.doc; *.docx` соответствует любому имени файла с расширением `doc` или `docx`.

- **Искать в** - Путь к папке, содержащей файлы для обработки. Это может быть локальная папка или сетевая папка. Сервер должен иметь достаточные права доступа для чтения файлов в этой папке. Чтобы указать сетевую папку, используйте ее UNC-путь (`\\server\share\folder`). Можно указать несколько папок, разделяя их пути точкой с запятой (;).
    - **Включая подкаталоги** - Если этот флажок установлен, задача будет обрабатывать файлы, содержащиеся как в папке, указанной в поле **Искать в**, так и во всех ее подпапках. В противном случае задача обрабатывает только файлы, содержащиеся непосредственно в указанной папке, без учета подпапок.
    - **Распаковывать архивы** - Если этот флажок установлен, задача будет обрабатывать файлы, содержащиеся в архивных файлах, например, в .zip-файлах. В противном случае задача обрабатывает архивные файлы таким же образом, как и любые другие двоичные файлы.
- **Изменен** - Когда этот флажок установлен, задача обрабатывает только файлы, которые соответствуют определенному условию, налагаемому на дату/время последнего изменения файла. Предусмотрены следующие условия:
    - **До** - Дата/время последнего изменения должны быть ранее указанных даты/времени.
    - **После** - Дата/время последнего изменения должны быть позднее указанных даты/времени.
    - **Между** - Дата/время последнего изменения должны быть в пределах указанного промежутка даты/времени.
    - **Не старше чем** - После даты/времени последнего изменения должно пройти не более указанного числа секунд, минут, часов, дней, недель, месяцев или лет.
    - **Старше чем** - После даты/времени последнего изменения должно пройти более указанного числа секунд, минут, часов, дней, недель, месяцев или лет.
- **Размер** - Когда этот флажок установлен, задача обрабатывает только файлы, которые соответствуют определенному условию, налагаемому на размер файла. Предусмотрены следующие условия:
    - **Равно** - Размер должен быть равен указанному значению.
    - **Меньше чем** - Размер должен быть меньше указанного значения.
    - **Больше чем** - Размер должен быть больше указанного значения.
    - **Между** - Размер должен быть между двумя указанными значениями.
- **Атрибуты** - Когда этот флажок установлен, задача обрабатывает только файлы с указанными атрибутами. Можно указать атрибуты файловой системы NTFS, такие как **Системный**, **Скрытый** и/или **Шифрованный**.

Управление существующими задачами

Для просмотра задач, относящихся к определенной классификации, выберите эту классификацию в дереве консоли под узлом **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **Задачи отпечатков**. На панели сведений предоставляется следующая информация по каждой задаче:

- **Имя задачи** - Имя, идентифицирующее задачу.
- **Статус** - Одно из следующих значений:
  - **Выполняется (X из Y файлов обработано)** - Задача исполняется. В скобках указывается количество файлов, обработанных задачей на данный момент (X), и общее количество файлов, подлежащих обработке (Y).
  - **Ожидает** - Задача включена (активна) и ожидает следующего автоматического запуска или запуска по расписанию.
  - **Неактивна** - Задача выключена (неактивна) и может быть запущена только вручную.

    Задача включена, если у нее установлен флажок **Активно**. Если задача включена, ее следующий запуск определяется параметром **Расписание**. Подробнее об этих параметрах см. в разделе Диалоговое окно для настройки задачи.
- **Время последнего обновления** - Дата и время последнего запуска задачи.
- **Добавлено отпечатков** - Количество отпечатков, созданных задачей во время последнего запуска. В скобках указывается общее количество созданных отпечатков по всем запускам этой задачей.
- **Обновлено отпечатков** - Количество отпечатков, обновленных задачей во время последнего запуска. Под обновлением подразумевается добавление новых версий и/или новых источников для отпечатков, уже имеющихся в базе данных.
- **Расписание** - Одно из следующих значений:
  - **Обновлять автоматически**, если у задачи выбран параметр **Обновлять автоматически при изменении содержимого директории**.
  - Дата и время следующего запуска, если у задачи выбран параметр **Обновлять каждые** <число> **минут**.

В верхней части панели сведений отображается список задач. Нижняя часть панели сведений содержит отчеты о выполнении задачи, выбранной в этом списке. В отчетах представлена история выполнения задачи, а также сведения об источниках отпечатков, которые были обработаны во время каждого запуска задачи. Подробнее см. в разделе Просмотр отчетов о выполнении задач.

Контекстное меню классификации в дереве консоли предоставляет следующие команды:

- **Создать задачу** - Создать и настроить новую задачу для данной классификации (см. Создание задач).
- **Обновить** - Обновить список задач выбранной классификации с учетом последних изменений. Эта команда не обновляет отчеты о выполнении задач. Для обновления отчетов о выполнении какой-либо задачи используйте команду **Обновить** из меню этой задачи на панели сведений.

Контекстное меню задачи в списке на панели сведений предоставляет следующие команды:

- **Запустить сейчас** - Запустить выбранную задачу. Эта команда позволяет запустить задачу вручную, независимо от ее расписания.
- **Создать задачу** - Создать и настроить новую задачу для той же классификации, что и выбранная задача (см. Создание задач).
- **Редактировать задачу** - Просмотреть или изменить параметры выбранной задачи. Эта команда открывает диалоговое окно, в котором можно просмотреть или изменить имя задачи, расписание и другие параметры (см. Диалоговое окно для настройки задачи).

- **Удалить задачу** - Удалить выбранную задачу. Удаление задачи не приводит к удалению отпечатков, созданных этой задачей. Информацию о том, как просмотреть и, при необходимости, удалить отпечатки из базы данных, см. в разделе База отпечатков.
- **Очистить историю** - Удалить все отчеты о выполнении выбранной задачи. Команда запрашивает подтверждение удаления и оставляет вместо удаленных отчетов сообщение о том, сколько отчетов было удалено, а также кем и с какого компьютера было выполнено удаление.
- **Обновить** - Обновить отчеты об выполнении выбранной задачи с учетом последних изменений. Эта команда не обновляет список задач на панели сведений. Чтобы обновить список задач какой-либо классификации, используйте команду **Обновить** на этой классификации в дереве консоли.

Просмотр отчетов о выполнении задач

Когда выбрана одна из классификаций под узлом **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **Задачи отпечатков** в дереве консоли, в верхней части панели сведений отображается список задач, которые обрабатывают отпечатки для данной классификации. В нижней части содержатся отчеты о выполнении задачи, выбранной в этом списке.

В нижней части панели сведений перечисляются запуски задачи в хронологическом порядке, так что последний запуск отображается первым в списке. Учитываются только те запуски, которые внесли существенные изменения в базу данных (например, добавление отпечатков). Прочие (непродуктивные) запуски задачи в список не включаются.

Для каждого запуска задачи, включенного в список, предоставляются следующие сведения:

- Заголовок отчета о запуске, состоящий из следующих элементов:
  - <дата-время начала> - <дата-время завершения>

    Эти элементы заголовка указывают дату и время начала и завершения задачи.
  - Способ запуска задачи:
    - **По расписанию** - Запуск по расписанию. У задачи выбран параметр **Обновлять каждые** <число> **минут**.
    - **Автоматически** - Запуск, вызванный изменением содержимого папки. У задачи выбран параметр **Обновлять автоматически при изменении содержимого директории**.
    - **Вручную** - Запуск по команде из консоли управления.
- Список файлов, обработанных задачей во время данного запуска, со следующей информацией о каждом файле:
  - **Имя файла** - Имя файла, обработанного задачей.
  - **Классификации: %** - Список классификаций, содержащих отпечатки, частично или полностью соответствующие отпечатку файла. Для каждой классификации в списке отображается процент соответствующих ей элементов отпечатка данного файла.
  - **Полный путь** - Полный путь к файлу. Если файл содержится в архиве, этот путь состоит из полного пути к файлу архива и пути к файлу внутри архива.

Управление классификациями

Каждая классификация может рассматриваться как контейнер, в котором хранятся цифровые отпечатки информации, отнесенной к определенному уровню важности или секретности. Классификации упорядочиваются в соответствии с этим уровнем. Если данный образец информации соответствует отпечаткам из нескольких классификаций, то считается, что он относится к классификации самого низкого уровня.

DeviceLock предоставляет следующие встроенные классификации:

- Совершенно секретно (высший уровень)
- Секретно
- Конфиденциально
- Для служебного пользования
- Открытая информация (низший уровень)

Изменить этот порядок встроенных классификаций нельзя; однако при необходимости можно добавить пользовательские классификации и установить для них желаемый порядок среди встроенных классификаций. При этом любую классификацию нельзя опустить ниже уровня классификации "Открытая информация".

Чтобы добавить, просмотреть или изменить пользовательские классификации, используется команда **Редактировать классификации** из меню узла **Задачи отпечатков**. Например, выберите **DeviceLock Enterprise Server** > **Цифровые отпечатки** в дереве консоли, щелкните правой кнопкой мыши **Задачи отпечатков** на панели сведений и выберите команду **Редактировать классификации** в контекстном меню.

Команда **Редактировать классификации** вызывает диалоговое окно, в котором можно:

- Просмотреть упорядоченный список всех классификаций (как встроенных, так и пользовательских), которые имеются в данный момент на сервере.
- Создать пользовательскую классификацию. Нажмите кнопку **Добавить** и введите имя для новой классификации.
- Изменить уровень пользовательской классификации. Выберите классификацию в списке и используйте кнопки со стрелками "вверх" и "вниз", расположенные рядом с кнопкой **Переименовать**.
- Изменить имя пользовательской классификации. Выберите классификацию в списке, нажмите кнопку **Переименовать** и введите новое имя.
- Удалить пользовательскую классификацию. Выберите классификацию в списке и нажмите кнопку **Удалить**.

> **Внимание:** При удалении пользовательской классификации автоматически удаляются все задачи и отпечатки, относящиеся к этой классификации.

DeviceLock не позволяет удалять и переименовывать встроенные классификации, а также изменять их порядок следования. Встроенная классификация "Открытая информация" всегда имеет самый низкий уровень.

База отпечатков

Сервер DeviceLock Enterprise Server хранит цифровые отпечатки предоставленных ему образцов информации (таких как документы и файлы) в базе данных отпечатков, и позволяет управлять отпечатками, хранящимися в этой базе данных. Отпечатки группируются согласно классификации их источника. Например, отпечатки, создаваемые задачей классификации "Секретно", попадают в классификацию "Секретно".

Список всех классификаций отпечатков, имеющихся в базе данных, отображается на панели сведений, если в дереве консоли выбран узел **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **База отпечатков**. По каждой классификации в этом списке приводятся следующие сведения:

- **Классификация** - Имя классификации.
- **Количество** - Количество отпечатков в базе данных, относящихся к данной классификации.
- **Размер** - Общий размер отпечатков, относящихся к данной классификации, в базе данных.
- **Время последнего обновления** - Дата и время последнего добавления или обновления отпечатков в данной классификации.
- **Обновление выполнено** - Имя задачи, которая последней добавила или обновила отпечатки в данной классификации. Если последним изменением в этой классификации было добавление отпечатков вручную, вместо имени задачи отображается имя учетной записи пользователя, добавившего отпечатки.
- **Частота срабатывания** - Счетчик, показывающий, сколько раз отпечатки из данной классификации срабатывали при проверке контента правилами на основе отпечатков.

  Этот счетчик увеличивается на единицу каждый раз, когда какое-либо правило обнаруживает, что проверяемый контент соответствует хотя бы одному отпечатку из данной классификации. При обработке такого правила счетчик увеличивается только на единицу, даже если проверяемый контент соответствует нескольким отпечаткам из данной классификации.
- **Эффективность классификации** - Процент, показывающий, сколько раз срабатывали отпечатки из данной классификации по сравнению с общим количеством срабатываний отпечатков по всем классификациям.

  Поскольку у одного и того же отпечатка могут быть элементы, относящиеся к разным классификациям, сумма показателей эффективности по всем классификациям может превышать 100%.

Контекстное меню классификации предоставляет следующие команды:

- **Добавить отпечаток** - Выбрать образец информации, например документ или файл, с которого требуется снять отпечаток. Отпечаток выбранного образца будет добавлен в классификацию, для которой выполняется эта команда (см. Добавление отпечатков вручную).
- **Обновить** - Обновить список на панели сведений учетом последних изменений.

  Эти команды имеются также в контекстном меню каждой классификации под узлом **База отпечатков** в дереве консоли (см. Просмотр списка отпечатков).

Управление отпечатками в базе данных предполагает:

- Просмотр списка отпечатков
- Просмотр подробной информации об отпечатках
- Добавление отпечатков вручную

Просмотр списка отпечатков

Все классификации отпечатков, имеющиеся в базе данных, перечислены в дереве консоли под узлом **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **База отпечатков**. Для просмотра отпечатков, относящихся к определенной классификации, выберите эту классификацию под узлом **База отпечатков** в дереве консоли.

Список отпечатков отображается на панели сведений, где предоставляются следующие сведения по каждому отпечатку:

- **Имя** - Имя, идентифицирующее отпечаток. При добавлении отпечатка файла в базу данных ему присваивается имя файла.

  Примечание: Запись в скобках после имени отпечатка, добавленного вручную, указывает кто и с какого компьютера добавил этот отпечаток (см. также Добавление отпечатков вручную).

- **Соответствие (%)** - Процент элементов отпечатка (хэшей), соответствующих выбранной классификации.

  Некоторые элементы отпечатка могут входить в состав других отпечатков, относящих к классификациям более низкого уровня. Так, отпечаток, помещенный в классификацию "Секретно", может быть получен из документа, часть которого служит источником другого отпечатка, включенного в классификацию "Открытая информация". В этом случае некоторые элементы отпечатка из классификации "Секретно" будут относиться к классификации "Открытая информация". Элементы, отнесенные к классификации более низкого уровня, не считаются соответствующими классификации более высокого уровня, поэтому соответствие может составлять менее 100%.

  Примечание: При вычислении соответствия оцениваются хэши всех версий данного отпечатка. В результате это значение для отдельной версии отпечатка (например, для его последней версии) может быть выше, чем для всего отпечатка.

- **Дата добавления** - Дата и время создания отпечатка.
- **Дата обновления** - Дата и время последнего обновления отпечатка.

  Обновление отпечатка происходит каждый раз, когда добавляется новая версия и/или новый источник отпечатка.

- **Версии** - Количество версий данного отпечатка, существующих в базе данных.
- **Источники** - Общее количество зарегистрированных источников данного отпечатка, при этом в скобках указывается количество "активных" источников. Источник считается активным, если он существует (не был удален, перемещен или переименован) и регулярно сканируется какой-либо задачей снятия отпечатков.
- **Тип источника** - Тип источника отпечатка:
  - **Текст** - В источнике имеется только текстовый контент (например, это текстовый файл). Отпечаток снимается с текстового контента.
  - **Бинарный** - В источнике нет текстового контента (например, это файл изображения). Отпечаток снимается с двоичных данных источника.
  - **Текст/Бинарный** - В источнике имеется как текстовый, так и двоичный контент (например, это документ Microsoft Word или файл .pdf). Отпечаток снимается с контента каждого типа отдельно.
- **Размер** - Размер отпечатка в базе данных.

- **Частота срабатывания** - Счетчик, показывающий, сколько раз данный отпечаток срабатывал при проверке контента правилами на основе отпечатков.

  Этот счетчик увеличивается на единицу в любом из следующих случаев:

  - Какое-либо правило с включенным параметром **Точное совпадение файла** обнаруживает, что контрольная сумма проверяемого контента совпадает с контрольной суммой файла-источника этого отпечатка.

    Примечание: Такое правило может не сработать, если в классификации нет ни одного элемента данного отпечатка (**Соответствие** отпечатка классификации равно нулю). Тем не менее при совпадении контрольных сумм счетчик увеличивается на единицу для классификации, содержащей данный отпечаток.

  - Какое-либо правило с заданным параметром **Порог** (параметр **Точное совпадение файла** выключен) обнаруживает любое из следующих условий:

    - Процент соответствия проверяемого контента данному отпечатку превышает значение параметра **Порог версионности для текста** или **Порог версионности для бинарных данных** (см. Настройки отпечатков).
    - Данный отпечаток наиболее соответствует проверяемому контенту по количеству совпадающих элементов (хэшей) в сравнении с другими отпечатками, имеющимися в базе данных.

    При этих условиях счетчик увеличивается на единицу независимо от того, сработало ли правило проверки контента.

  Примечание: В любом из перечисленных выше случаев счетчик увеличивается во всех классификациях, которым соответствует данный отпечаток.

- **Эффективность** - Процент, показывающий, сколько раз данный отпечаток срабатывал при проверке контента правилами на основе отпечатков по сравнению с общим количеством срабатываний отпечатков этой классификации.

Контекстное меню классификации в дереве консоли предоставляет следующие команды:

- **Добавить отпечаток** - Выбрать образец информации, например документ или файл, с которого требуется снять отпечаток. Отпечаток выбранного образца будет добавлен в классификацию, для которой выполняется эта команда (см. Добавление отпечатков вручную).
- **Обновить** - Обновить список отпечатков выбранной классификации с учетом последних изменений. Эта команда не обновляет подробную информацию, отображаемую под списком отпечатков. Чтобы обновить информацию о каком-либо отпечатке, используйте команду **Обновить** из меню этого отпечатка на панели сведений.

Контекстное меню отпечатка в списке на панели сведений предоставляет следующие команды:

- **Добавить отпечаток** - То же, что и на классификации в дереве консоли.
- **Удалить отпечаток** - Удалить отпечаток, на котором выполняется эта команда.

  Команда **Удалить отпечатки**, которая появляется в случае выбора двух или более отпечатков, позволяет удалить сразу все выбранные отпечатки.

- **Обновить** - Обновить подробную информацию о выбранном отпечатке с учетом последних изменений (см. Просмотр подробной информации об отпечатках). Эта команда не обновляет список отпечатков на панели сведений. Чтобы обновить список отпечатков из какой-либо классификации, используйте команду **Обновить** на этой классификации в дереве консоли.

Просмотр подробной информации об отпечатках

Когда выбрана одна из классификаций под узлом **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **База отпечатков** в дереве консоли, в верхней части панели сведений отображается список отпечатков, отнесенных к данной классификации. В нижней части можно просмотреть информацию о версиях и источниках отпечатка, выбранного в этом списке.

Отпечатки, хранящиеся в базе данных, снимаются с определенных образцов информации (например, документов или файлов изображений), называемых источниками отпечатков. Эти источники регистрируются в базе данных при добавлении или обновлении отпечатков.

При первоначальном добавлении отпечатка его источник регистрируется как единственный источник этого отпечатка. Для отпечатков, уже имеющихся в базе данных, могут быть зарегистрированы дополнительные источники. Так, для имеющегося отпечатка новый файл-источник регистрируется в следующих случаях:

- Обнаружено, что изменился путь или имя ранее зарегистрированного файла-источника. Данный файл регистрируется как новый источник с соответствующим путем и именем.
- Отпечаток некоторого файла добавлен в качестве версии имеющегося отпечатка, и этот файл не входит в число зарегистрированных источников этого отпечатка. Данный файл регистрируется как новый источник вместе с новой версией отпечатка.

Создав отпечаток, сервер может добавить его в базу данных в качестве нового отпечатка или как версию другого отпечатка, который уже существует в базе данных. Версия добавляется, если процент совпадающих элементов вновь созданного отпечатка и существующего отпечатка превышает пороговое значение, заданное соответствующей настройкой (см. Настройки отпечатков).

Различные версии отпечатка могут создаваться задачами разных классификаций, в результате чего элементы отпечатка распределяются между несколькими классификациями. Считается, что такой отпечаток соответствует нескольким классификациям с некоторым (отличным от нуля) процентом соответствия каждой классификации.

Примечание: При сопоставлении проверяемого контента с тем или иным отпечатком из базы данных выполняется сравнение с элементами (хэшами) всех версий отпечатка.

В консоли предоставляются следующие сведения о версиях и источниках каждого отпечатка:

- **Версия** - Номер версии. Первоначально отпечаток имеет единственную версию с номером 1. Добавление каждой новой версии увеличивает номер версии на единицу.

  При необходимости можно удалять отдельные версии отпечатка. Для этого следует нажать красный крестик в столбце **Удалить** рядом с номером версии в списке.

- **Путь** - Полный путь и имя источника отпечатка. Это может быть путь на локальном диске или UNC-путь на сетевом файловом сервере. Если источник содержится в архиве, его полный путь состоит из пути к файлу архива и пути к источнику внутри архива.

  Некоторые версии могут содержать элементы отпечатков (хэши) нескольких источников. В этом случае имена и пути всех таких источников перечисляются в столбце **Путь** рядом с номером версии.

Цвет значка в столбце **Путь** указывает состояние источника отпечатка:

- Зеленый - Означает, что источник с указанным путем и именем существует и регулярно сканируется какой-либо задачей снятия отпечатков.
- Серый - Появляется в следующих случаях:
  - Отпечаток данного источника был снят вручную (см. Добавление отпечатков вручную).
  - Источник с указанным путем и именем больше не существует (например, файл-источник был переименован, перемещен или удален).
  - Сканирование данного источника задачами снятия отпечатков больше не выполняется по причине изменений в параметрах задач (эти параметры описаны в разделе Диалоговое окно для настройки задачи).

- **Дата добавления** - Дата и время последнего добавления отпечатков указанного источника в базу данных.
- **Время последнего сканирования** - Дата и время выполнения последнего сканирования данного источника задачами снятия отпечатков.
- <Имя классификации> **(%)** - Процент элементов (хэшей) отпечатка, соответствующих указанной классификации. В списке может быть несколько имен, т.к. различные элементы отпечатка могут соответствовать разным классификациям.

Добавление отпечатков вручную

Как правило, база данных отпечатков заполняется при помощи задач (см. Задачи отпечатков). Предусмотрена также возможность добавлять отпечатки напрямую, без необходимости создавать, настраивать и запускать задачу. Эта функция предназначена для оперативного снятия отпечатков файлов и сохранения их в базе данных.

Чтобы оперативно снять и сохранить отпечатки, используйте команду **Добавить отпечаток**, имеющуюся на каждой классификации в узле консоли База отпечатков. Отпечатки будут добавлены в классификацию, для которой выполняется эта команда. Команда предлагает выбрать файлы, а затем сервер снимает и сохраняет отпечатки этих файлов в базе данных.

Команда **Добавить отпечаток** использует стандартное диалоговое окно для выбора файлов, дополненное флажком, который действует, если выбран файл архива (например, .zip-файл):

- **Распаковывать архивы** - Если этот флажок установлен, отпечаток снимается с каждого файла, содержащегося в архиве. В противном случае архив обрабатывается таким же образом, как и любой двоичный файл, и отпечаток будет снят только с самого файла архива.

По завершении команды появляется диалоговое окно со списком добавленных отпечатков, в котором предоставляются следующие сведения по каждому отпечатку:

- **Имя** - Имя, идентифицирующее отпечаток. При добавлении отпечатка в базу данных сервер присваивает ему имя файла, с которого этот отпечаток был снят.
- **Тип источника** - Тип файла для снятия отпечатка или прочерк в случае пустого файла. Возможны следующие типы:
  - **Текст** - В файле имеется только текстовый контент (например, это текстовый файл). Отпечаток снимается с текстового контента.
  - **Бинарный** - В файле нет текстового контента (например, это файл изображения). Отпечаток снимается с двоичных данных источника.
  - **Текст/Бинарный** - В файле имеется как текстовый, так и двоичный контент (например, это документ Microsoft Word или файл .pdf). Отпечаток снимается с контента каждого типа отдельно.

- <Имя классификации> - Процент элементов (хэшей) отпечатка, соответствующих указанной классификации. В списке может быть несколько имен, поскольку различные отпечатки и их отдельные элементы могут соответствовать различным классификациям.
- **Полный путь** - Путь и имя файла, с которого данный отпечаток был снят. Это может быть путь на локальном сервере или UNC-путь на сетевом файловом сервере. Если файл содержится в архиве, отображается путь к архиву и путь к файлу внутри архива.
- **Информация** - Результат операции:
    - **Добавлен** - Отпечаток успешно снят и сохранен в базе данных.
    - **Добавлен, Поврежденные данные** - Не удалось снять отпечаток текстового контента, возможно, из-за повреждения текстовых данных. Отпечаток снят только с двоичных данных.
    - **Добавлен, Защищено паролем** - Не удалось снять отпечаток текстового контента, т.к. текстовые данные защищены паролем. Отпечаток снят только с двоичных данных.
    - **Уже существует** - Отпечаток данного файла уже есть в базе данных.
    - **Пусто** - Файл для снятия отпечатка не содержит данных. Отпечаток не создан.
    - **Ошибка:** <сообщение> - Сообщение об ошибке, если снять отпечаток по какой-то причине не удалось.

Журнал отпечатков

В журнале отпечатков хранятся записи, которые помогают отслеживать события, связанные с управлением и обработкой отпечатков на сервере DeviceLock Enterprise Server. В журнале регистрируются события, вызванные следующими действиями:

- Изменение связанных с отпечатками настроек сервера, таких как пороги создания версий (см. Настройки отпечатков) или пользовательские классификации (см. Управление классификациями).
- Действия по управлению задачами создания отпечатков (см. Задачи отпечатков), такие как запуск, завершение, добавление, изменение или удаление задач, или удаление отчетов о выполнении задач.
- Добавление отпечатков задачами их создания (см. Задачи отпечатков) или вручную (см. Добавление отпечатков вручную).
- Удаление отпечатков и/или их версий (см. Просмотр списка отпечатков, Просмотр подробной информации об отпечатках).
- Обработка связанных с отпечатками клиентских запросов, таких как проверка отпечатков по запросу сервиса DeviceLock или агента Discovery (см. Применение цифровых отпечатков). Журнал предоставляет информацию о запуске и завершении обработки, а также об ошибках в случае их появления при обработке запроса.

Информация, хранимая в данном журнале, позволяет отслеживать изменения параметров и задач управления отпечатками, а также помогает обнаруживать и устранять проблемы, связанные с управлением отпечатками и их применением.

Для просмотра журнала выберите **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **Просмотрщик журнала отпечатков** в дереве консоли. На панели сведений консоли отображается список событий, зарегистрированных в журнале отпечатков, со следующими сведениями по каждому событию:

- **Тип** - Возможны события следующих типов:
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- **Дата/Время** - Дата и время события.
- **Событие** - Идентификационный номер события.
- **Имя задачи** - Задачи снятия отпечатков, вызвавшая событие или затронутая этим событием.
- **Имя классификации** - Классификация отпечатков, относящаяся к событию или затронутая этим событием.
- **Информация** - Описание события, в том числе описание действий и ошибок.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, который зарегистрировал данное событие.
- **Запись N** - Порядковый номер события в списке.
- **Сервер консолидации** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов (см. Консолидация журналов).
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов (см. Консолидация журналов).

Управление журналом отпечатков

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узлы **DeviceLock Enterprise Server** > **Цифровые отпечатки** и щелкните правой кнопкой мыши элемент **Просмотрщик журнала отпечатков** под узлом **Цифровые отпечатки**.

  - или -

- В дереве консоли DeviceLock Management Console выберите **DeviceLock Enterprise Server** > **Цифровые отпечатки** > **Просмотрщик журнала отпечатков** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное количество записей в журнале.
- **Сохранить** - Сохранить журнал в указанный файл.
- **Обновить** - Обновить список событий с учетом последних изменений.
- **Фильтр** - Задать условия фильтрации списка событий.
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра событий, произошедших за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).
- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи о событиях, имеющиеся в журнале на данный момент.

  Эта команда добавляет в журнал запись об удалении, указывающую, сколько записей было удалено, а также кто выполнил удаление и с какого компьютера.

Чтобы просмотреть или изменить настройки журнала

1. Выберите команду **Настройки** в контекстном меню.
2. Используйте параметры, представленные в появившемся диалоговом окне (см. Настройки журнала отпечатков).

Чтобы настроить фильтр журнала

1. Выберите команду **Фильтр** в контекстном меню.
2. Используйте параметры, представленные в появившемся диалоговом окне (см. Фильтр журнала отпечатков).

Настройки журнала отпечатков

Диалоговое окно для управления настройками журнала отпечатков позволяет просмотреть или изменить следующие параметры:

- **Контролировать размер журнала** - Установите этот флажок, чтобы контролировать количество записей в журнале и удалять устаревшие записи. Если этот флажок не установлен, для хранения журнала используется все доступное дисковое пространство.
- **Сохранять события за последние** <число> **дней** - Если выбран этот параметр, в журнале хранятся записи не старше заданного количества дней (по умолчанию - 365 дней).
- **Максимальный размер:** <число> **записей** - Если выбран этот параметр, в журнале хранится не более заданного количества записей. Для данного параметра необходимо выбрать, какое действие будет выполняться при достижении максимального размера журнала:
    - **Затирать старые события по необходимости** - Новые записи событий продолжают сохраняться при достижении максимального размера журнала. Каждая запись нового события заменяет собой самую старую запись в журнале.
    - **Затирать события старше** <число> **дней** - Новые записи событий заменяют собой только записи, хранящиеся дольше заданного количества дней. Поддерживаемая настройка - до 32 767 дней.
    - **Не затирать события (очистка журнала вручную)** - При достижении максимального размера журнала новые записи событий не добавляются. Чтобы обеспечить их добавление, необходимо вручную удалить старые записи.

Примечание: Сервер удаляет старые записи по дате, указанной в столбце **Дата/Время** (если запись была выполнена локальным сервером), либо по дате, указанной в столбце **Дата/Время консолидации** (если запись была получена от другого сервера посредством консолидации).

Внимание: Если в журнале нет места для новых записей, а настройки журнала не позволяют удалить старые записи, сервер не будет добавлять новые записи в журнал.

Чтобы использовать настройки по умолчанию, нажмите кнопку **Восстановить умолчания**. В результате будут установлены следующие настройки:

- Максимальный размер: 10 000 записей
- Затирать события старше 7 дней

Фильтр журнала отпечатков

В результате применения фильтра консоль отображает только записи о событиях, которые соответствуют условиям, заданным в диалоговом окне для управления фильтром журнала отпечатков.

Предусмотрены два типа фильтра:

- **Включить** - Отображать только записи о событиях, которые соответствуют заданным условиям. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Включить** и задайте условия на этой вкладке.
- **Исключить** - Не отображать записи о событиях, которые соответствуют заданным условиям. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Исключить** и задайте условия на этой вкладке.

Фильтр можно временно выключить. Для этого снимите флажок **Включить фильтр**.

Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

Когда фильтр включен, можно задать условия фильтрации, задав необходимые значения в следующих полях:

- **Типы событий** - Фильтрация по типу событий. Возможны следующие варианты (установите соответствующие флажки):
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- Строковые поля, предназначенные для включения или исключения из списка записей о событиях, у которых в указанном поле данных встречается заданная строка. Например, для фильтрации записей по имени задачи, вызвавшей событие, укажите строку фильтра в поле **Имя задачи**. Для фильтрации записей о событиях с определенными номерами, введите номера искомых событий в поле **ID-события**, разделяя их точкой с запятой.

  Предусмотрены следующие строковые поля:

  - **Имя классификации** - Имя классификации отпечатков, относящейся к событию или затронутой этим событием.
  - **Имя задачи** - Имя задачи снятия отпечатков, вызвавшей событие или затронутой этим событием.
  - **Информация** - Описание события, в том числе описание действий и ошибок.
  - **Сервер** - Имя сервера DeviceLock Enterprise Server, зарегистрировавшего событие.
  - **ID-события** - Идентификационный номер события.

  Примечание: Чтобы облегчить настройку фильтра, строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

- **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были зарегистрированы сервером.
- **Консолидация** - Поля для фильтрации по данным, относящимся к консолидации журналов (см. Консолидация журналов):
  - **Сервер** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов. Это поле нечувствительно к регистру и позволяет использовать знаки подстановки (* и ?). Используя точку с запятой в качестве разделителя, можно задать несколько значений.
  - **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были последний раз получены с удаленного сервера при консолидации журналов.

Для каждого временного диапазона предусмотрены следующие настройки:

- **С** - Начало диапазона. Возможные значения:
  - **Первой записи** - Фильтровать события, начиная с самой ранней даты и времени в соответствующем поле журнала.
  - **Записи от** - Фильтровать события, начиная с определенной даты и времени.
- **По** - Конец диапазона. Возможные значения:
  - **Последнюю запись** - Фильтровать события, заканчивая самой поздней датой и временем в соответствующем поле журнала.
  - **Записи от** - Фильтровать события, заканчивая определенной датой и временем.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

Применение цифровых отпечатков

Чтобы использовать цифровые отпечатки, вначале собирают образцы документов и файлов, которые требуется защитить, и классифицируют их на сервере DeviceLock Enterprise Server с помощью задач, выполняющих снятие отпечатков (см. Управление цифровыми отпечатками).

Чтобы настроить сервис DeviceLock для применения правил, основанных на цифровых отпечатках, требуется:

- Указать один или несколько серверов DeviceLock Enterprise Server, на которых размещена база данных отпечатков. Инструкции см. в разделе Настройки сервиса для цифровых отпечатков.
- Создать и настроить контентные группы на основе отпечатков. Инструкции см. в разделе Группы цифровых отпечатков.
- Используя эти группы, настроить правила проверки контента, как описано в разделе Контентно-зависимые правила (обычный профиль) ранее в этом документе.

Настройки сервиса для цифровых отпечатков

Чтобы использовать метод цифровых отпечатков, требуется взаимодействие между сервисом DeviceLock и сервером DeviceLock Enterprise Server. Это связано с тем, что база данных отпечатков находится на сервере, тогда как правила проверки отпечатков применяются на клиентских компьютерах (см. Сравнение отпечатков).

В настройках сервиса имеются параметры, определяющие сервер для проверки отпечатков. Эти параметры отображаются на панели сведений, если в дереве консоли выбрать **Сервис DeviceLock** > **Настройки сервиса** > **Цифровые отпечатки**.

Предусмотрены следующие параметры:

- Использовать глобальную настройку DeviceLock Enterprise Server(ы) - Для проверки отпечатков использовать тот же сервер (или серверы), что и для других операций (например, сбора журналов аудита и теневого копирования или управления политиками).

  Внимание: Будут использоваться только серверы, указанные для учетной записи “Все” (Everyone).

- DeviceLock Enterprise Server(ы) - Использовать выделенные серверы для проверки отпечатков.

В случае авторизации по сертификату, когда для сервиса DeviceLock установлен открытый ключ сертификата DeviceLock, на сервере, предназначенном для проверки отпечатков, должен быть установлен закрытый ключ этого сертификата, как описано в разделе Администраторы сервера и сертификат. В противном случае правила, основанные на отпечатках, действовать не будут (подробнее см. в разделе Если серверная база данных отпечатков недоступна).

Использовать глобальную настройку DeviceLock Enterprise Server(ы)

Чтобы включить или отключить этот параметр, дважды щелкните его на панели сведений.

Когда этот параметр включен, для проверки отпечатков используются серверы, указанные для учетной записи “Все” (Everyone) в параметре **Настройки сервиса** > DeviceLock Enterprise Server(ы).

Когда этот параметр отключен, для проверки отпечатков используются серверы, указанные в параметре **Настройки сервиса** > **Цифровые отпечатки** > DeviceLock Enterprise Server(ы).

DeviceLock Enterprise Server(ы)

Чтобы включить этот параметр для проверки отпечатков на выделенных серверах DeviceLock Enterprise Server, нужно отключить параметр Использовать глобальную настройку DeviceLock Enterprise Server(ы). В противном случае параметр **DeviceLock Enterprise Server(ы)** недоступен.

Если этот параметр включен, то для проверки отпечатков сервис DeviceLock использует серверы, перечисленные в этом параметре. Дважды щелкните параметр на панели сведений; затем используйте появившееся диалоговое окно, чтобы просмотреть или изменить список серверов.

Чтобы добавить сервер в список, введите имя компьютера, на котором установлен DeviceLock Enterprise Server. Это может быть полное доменное имя (FQDN), короткое имя или IP-адрес компьютера. Чтобы добавить несколько серверов, введите имена компьютеров, разделенные точкой с запятой (;).

Можно изменить или удалить отдельные имена компьютеров из списка. Чтобы очистить список, нажмите кнопку **Удалить**.

Группы цифровых отпечатков

Контентные группы цифровых отпечатков реализуют проверку контента с использованием цифровых отпечатков. Каждая группа такого типа ссылается на определенную классификацию цифровых отпечатков и определяет минимальный процент соответствия отпечатков (называемый порогом), который требуется для присвоения данной классификации проверяемому контенту.

Контентно-зависимые правила могут использовать контентные группы цифровых отпечатков для анализа данных на основе цифровых отпечатков. Такие правила могут применяться как к устройствам, так и к сетевым протоколам, с целью использовать цифровые отпечатки для управления разрешениями на доступ к контенту, теневым копированием контента и/или обнаружением контента.

Для создания группы цифровых отпечатков требуется выполнить следующие действия:

1. Открыть диалоговое окно для управления контентно-зависимыми правилами. О том, как открыть это окно, см. раздел Редактирование или удаление пользовательских контентных групп ранее в этом документе.
2. В диалоговом окне для управления контентно-зависимыми правилами в области **База данных контента** раскрыть список рядом с кнопкой **Добавить группу** и выбрать в нем пункт **Цифровые отпечатки**.
3. Настроить параметры группы в появившемся диалоговом окне (см. Диалоговое окно для настройки группы цифровых отпечатков).

Создав группу цифровых отпечатков, ее можно использовать наряду с другими контентными группами при настройке правил проверки контента, как описано в разделе Контентно-зависимые правила (обычный профиль) ранее в этом документе.

Диалоговое окно для настройки группы цифровых отпечатков

В диалоговом окне для настройки группы цифровых отпечатков можно просмотреть или изменить следующие параметры:

- **Имя** - Имя, позволяющее идентифицировать данную группу.
- **Описание** - Необязательный текст, который может описывать, например, назначение группы.
- **Сервер DeviceLock** - Имя компьютера, на котором работает сервер DeviceLock Enterprise Server (например, полное доменное имя (FQDN) этого компьютера). Этот параметр используется только для настройки группы и не влияет на применение и обработку правил на основе этой группы.

  Диалоговое окно получает список пользовательских классификаций с сервера, указанного в этом поле. Если на серверах DeviceLock Enterprise Server нет пользовательских классификаций или они не нужны для данной группы, это поле можно оставить пустым. В результате пользовательские классификации будут отсутствовать в списке поля **Классификация**, а кнопка **Получить** будет недоступна.
- **Классификация** - Имя классификации цифровых отпечатков для этой группы. Правила, использующие эту группу, проверяют представленную информацию, сопоставляя ее отпечатки с отпечатками из указанной классификации. Когда правило обнаруживает достаточное соответствие отпечатков, информации присваивается соответствующий уровень классификации.

  Список поля **Классификация** позволяет выбрать любую встроенную классификацию, кроме классификации “Открытая информация”. Список можно расширить путем добавления пользовательских классификаций, определенных на серверах DeviceLock Enterprise Server. Для этого заполните поле **Сервер DeviceLock** и нажмите кнопку **Получить**.

  Примечание: После того, как настройки будут применены и диалоговое окно будет закрыто, консоль сохранит указанное имя сервера, а пользовательские классификации с этого сервера будут автоматически добавлены в список при открытии этого диалогового окна в следующий раз.
- **Точное совпадение файла** - Если этот флажок установлен, группа определяет точное совпадение проверяемых файлов с файлами-источниками отпечатков из базы данных. Правило, использующее такую группу, обнаруживает совпадение двух файлов только в случае совпадения их контрольных сумм. Другие элементы (хэши) отпечатков этих файлов не сравниваются.

  Если некоторый файл в точности совпадает с файлом-источником, элементы отпечатка которого относятся к разным классификациям, то такому файлу присваивается самый высокий уровень этих классификаций. Например, если 10% отпечатка файла-источника относится к классификации “Совершенно секретно”, а остальные 90% - “Открытая информация”, то совпадающий с ним файл относится к классификации “Совершенно секретно”. В результате группа может не обнаружить точное совпадение файлов, если ее уровень классификации ниже наивысшего уровня классификации файла-источника.

  Если этот флажок снят, группа служит для сравнения других элементов (хэшей) отпечатка, что позволяет обнаруживать частичные совпадения проверяемого контента с содержимым источников отпечатков из базы данных. Степень соответствия отпечатков, которая указывает на частичное совпадение содержимого, определяется параметром **Порог**.

Примечание: Если у группы установлен флажок **Точное совпадение файла**, то:

- Группа сравнивает контрольную сумму проверяемого файла с контрольными суммами файлов-источников всех версий отпечатков из указанной классификации.
- Правила, использующие такую группу, могут не выполнять проверку отпечатков файлов, содержащихся в архиве. Подробнее см. в разделе Проверка отпечатков внутри архива.
- Разрешающее правило, основанное на такой группе, имеет приоритет над запрещающими правилами, разрешая передачу любого соответствующего этому правилу контента. Разрешающее правило, основанное на составной группе, будет иметь приоритет в том случае, когда логически связанная цепочка групп, разрешающая данный контент, имеет в своем составе группу, у которой установлен флажок **Точное совпадение файла**.

- **Порог** - Правило срабатывает, если процент информации, соответствующей выбранному уровню классификации, в проверяемом контенте превышает значение, заданное этим параметром. Процент информации, соответствующей данной классификации, определяется путем оценки того, как много элементов в отпечатке проверяемого контента соответствует отпечаткам этой классификации, хранящимся в базе данных. Более подробную информацию можно найти в разделе Как этот метод устроен (см. Процент соответствия).
- **Использовать только бинарные отпечатки для файлов, защищенных паролем** - Когда этот флажок установлен, группа не проверяет текстовый контент, если его невозможно извлечь из документа или архива по причине защиты паролем. Правило, использующее такую группу, проверяет отпечатки двоичного и, по возможности, текстового контента. Если DeviceLock не может извлечь текстовый контент, то правило ограничивается проверкой двоичного контента.

  Когда этот флажок снят, группа вызывает ошибку, если не может проверить текстовый контент защищенного паролем документа или архива. В таком случае сервис DeviceLock не разрешает этот документ или архив из-за ошибки при проверке его отпечатков.

7

Протоколы (обычный профиль)

В этой главе:

Общая информация

Разрешения на доступ к протоколам

Аудит, теневое копирование и алерты для протоколов

Белый список протоколов

Базовый IP-файрвол

Настройки безопасности для протоколов

Контроль трафика с SSL-шифрованием

Общая информация

DeviceLock дает возможность контролировать данные, передаваемые через различные сетевые протоколы, что существенно усиливает защиту от несанкционированных утечек информации и обеспечивает дополнительную защиту на транспортном уровне. Используя функциональность контроля доступа к сетевым протоколам, можно выборочно разрешить или запретить передачу файлов и данных через определенные протоколы, а также включить теневое копирование передаваемых данных. Имеется возможность задавать различные политики контроля доступа для различных пользователей и групп.

DeviceLock распознает и контролирует следующие протоколы:

- **Поиск работы** - Контролируется поиск вакансий на веб-сайтах поиска работы, включая контроль файлов, сообщений и поисковых запросов пользователей, обращающихся к таким сайтам. Обеспечивается контроль для веб-сайтов следующих поставщиков данной услуги (включая сайты в национальных доменах):
    - 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
- **Файловые хранилища** - Контролируется обмен данными через веб-хранилища (сетевые службы файлового обмена и синхронизации). Поддерживаются следующие веб-хранилища:
    - 4shared (в том числе контроль приложения 4shared для Windows)
    - Amazon Simple Storage Service (Amazon S3)
    - AnonFile
    - Box
    - dmca.gripe
    - Dropbox

      Примечание: Чтобы использовать приложение Dropbox для Windows, в белый список протоколов необходимо добавить правило для протокола SSL, в котором указаны следующие хосты:
      - *.dropbox.com
      - *.compute-1.amazonaws.com

      Инструкции см. в разделе Задание белого списка протоколов.
    - DropMeFiles
    - Easyupload.io
    - Files.fm
    - freenet.de
    - Служба файлового обмена GitHub

      Примечание: Для доступа к службе файлового обмена GitHub через Windows-приложения, такие как GitHub Desktop, SmartGit или TortoiseGit, в белый список протоколов необходимо добавить правило для протокола SSL, в котором указан хост github.com.

      Инструкции см. в разделе Задание белого списка протоколов.
    - Файловое хранилище GMX
    - Gofile.io
    - Google Docs / Google Drive

      Примечание: Чтобы использовать приложение Backup and Sync from Google (бывш. Google Drive Sync), в белый список протоколов необходимо добавить правило для протокола SSL, в котором указаны следующие хосты:
      - *accounts.google.com
      - *www.googleapis.com

      Инструкции см. в разделе Задание белого списка протоколов.

- iCloud
- IDrive
- MagentaCLOUD
- MediaFire
- MEGA (в том числе контроль приложения MEGAsync для Windows)

  Примечание: DeviceLock контролирует доступ к службе файлового обмена MEGA и загрузку файлов через эту службу (исходящие файлы). Контроль входящих файлов и POST-запросов для службы MEGA не выполняется.

- OneDrive
- Sendspace
- transfer.sh
- TransFiles.ru
- Uploadfiles.io
- Служба файлового обмена Web.de
- WeTransfer
- Облако Mail.ru
- Яндекс.Диск

  Примечание: Чтобы использовать приложение Яндекс.Диск для Windows, в белый список протоколов необходимо добавить правило для протокола SSL, в котором указаны следующие хосты:
  - webdav.yandex.ru
  - *downloader.disk.yandex.ru
  - uploader*.disk.yandex.net
  - push.yandex.ru
  - *.storage.yandex.net
  - oauth.yandex.ru
  - cloud-api.yandex.net

  Инструкции см. в разделе Задание белого списка протоколов.

DeviceLock осуществляет контроль веб-служб обмена файлами через HTTP, а также контролирует обмен файлами и данными через протокол WebDAV (Web Distributed Authoring and Versioning).

Поддерживаются как незащищенные, так и защищенные (SSL) соединения.

- **FTP** (протокол передачи файлов) - Стандартный протокол для передачи файлов с одного компьютера на другой через сеть Internet.

  Поддерживаются активный и пассивный режимы FTP-соединений, а также FTPS (FTP + SSL). Поддерживаются следующие типы FTPS: Implicit FTPS и Explicit FTPS.

- **HTTP** (протокол передачи гипертекста) - Протокол клиент-сервер прикладного уровня, используемый для передачи данных по World Wide Web.

  Контроль HTTP включает также контроль обмена данными через протокол WebDAV (Web Distributed Authoring and Versioning), являющийся расширением HTTP.

  Также поддерживается HTTPS (SSL + HTTP).

- **IBM Notes** - Проприетарный протокол, используемый IBM Notes для коммуникаций с сервером IBM Domino. DeviceLock поддерживает версию 8.5 (Декабрь 2008) и более поздние версии, с любыми клиент-серверными комбинациями Domino / Notes.

- **ICQ Messenger** - Открытый сетевой протокол OSCAR, обеспечивающий обмен сообщениями в реальном времени. Используется приложением ICQ Messenger.

  Поддерживаются незащищенные и защищенные (SSL) соединения.
- **IRC** (ретранслируемый интернет-чат) - Сервисная система, при помощи которой можно общаться через сеть Интернет с другими людьми в режиме реального времени.

  Поддерживаются незащищенные и защищенные (SSL) соединения.
- **Jabber** - Основанный на XML открытый протокол для мгновенного обмена сообщениями. Jabber также известен как XMPP (Extensible Messaging and Presence Protocol).
- **Mail.ru Агент** - Программа для быстрого обмена сообщениями через Интернет, разработанная компанией Mail.ru.

  Примечание: SSL-подключения между клиентами Jabber/Mail.ru Агент и сервером контролируются как обычные (generic) подключения без SSL.
- **MAPI** (Messaging Application Programming Interface) - MAPI/RPC (известный также как Outlook - Exchange Transport Protocol) представляет собой закрытый протокол для взаимодействия Microsoft Outlook и Microsoft Exchange Server. DeviceLock поддерживает все версии Outlook (как 32-разрядные, так и 64-разрядные), начиная с Outlook 2003. Также поддерживаются все версии Exchange Server.
- **Skype** - Проприетарная голосовая веб-служба и клиентское приложение. В рамках этого протокола DeviceLock контролирует коммуникации через следующие приложения:
  - Skype версии 4.x и выше
  - Skype для бизнеса (Skype for Business) 2015, 2016 или 2019
  - Microsoft Lync 2013
  - Собрания Skype (Skype Meetings App)
  - Skype для бизнеса (Skype for Business) Web App
  - Skype для бизнеса (Skype for Business) в Outlook Web App (OWA 365)

  Примечание: Коммуникации через MSN/Windows Messenger блокируются, если заданы разрешения, аудит, теневое копирование или алерты для протокола Skype.
- **SMB** (Server Message Block) - Сетевой протокол обмена файлами.
- **SMTP** (простой протокол передачи почты) - Сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

  Также поддерживается Extended SMTP (ESMTP). Поддерживаются незащищенные и защищенные (SSL) соединения.
- **Социальные сети** - Контролирует сайты социальных сетей. Поддерживаются следующие сайты социальных сетей:
  - Disqus
  - Facebook (+API)
  - Google+
  - Instagram (в т.ч. контроль приложения Instagram для Windows 10)
  - LinkedIn
  - LiveInternet.ru
  - LiveJournal
  - MeinVZ.de
  - Myspace

    - Odnoklassniki.ru
    - Pinterest
    - StudiVZ.de
    - Tumblr
    - Twitter
    - Vkontakte (+API)
    - XING.com

    Примечание: SSL-трафик сайтов социальных сетей контролируется как обычный (generic).

- **Telegram** - Контролирует программы обмена сообщениями Telegram Desktop (в том числе приложение Telegram Desktop для Windows 10) и Telegram Web.
- **Telnet** - Сетевой протокол для реализации текстового интерфейса по сети.
- **Торрент** - Контролирует P2P-коммуникации торрент-клиентов по протоколам TCP, UDP или HTTP.
- **Viber** – Служба и клиентское приложение для обмена мгновенными сообщениями и передачи голоса по IP. DeviceLock поддерживает Windows-приложение Viber версии 4.x и выше.
- **Web-почта** - Контролирует почтовые веб-службы. Поддерживаются следующие почтовые веб-службы:
    - ABV Mail
    - AOL Mail
    - freenet.de
    - Gmail
    - GMX Mail
    - Hotmail (Outlook.com)
    - Mail.ru
    - NAVER
    - Outlook Web App (OWA)
    - Rambler Mail
    - T-online.de
    - Web.de
    - Yahoo! Mail
    - Yandex Mail
    - Zimbra

    Поддерживаются как незащищенные, так и защищенные (SSL) соединения.

    Примечание: Если протокол HTTP не разрешен настройками разрешений для протоколов, возможны сбои при подключении к почтовой службе Zimbra или Outlook Web App (OWA), несмотря на разрешение протокола Web-почта. Для предотвращения сбоев в такой ситуации внесите хосты Zimbra и OWA в белый список для протокола HTTP. Инструкции см. в разделе Действия по управлению белым списком.

- **Web-поиск** - Контролируется использование веб-сайтов, предоставляющих услуги поиска в интернете, а также поисковые запросы пользователей на таких сайтах. Обеспечивается контроль для сайтов следующих провайдеров веб-поиска (включая сайты в национальных доменах и мобильные версии сайтов):
    - 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** - Контролирует веб-приложение WhatsApp Web, а также приложение WhatsApp Desktop для компьютеров под управлением Windows.
- **Zoom** - Облачная платформа для видео- и аудиоконференцсвязи, чатов и вебинаров, предоставляемая компанией Zoom Video Communications. В рамках данного протокола контролируется использование клиентского приложения Zoom для компьютеров под управлением Windows, в том числе установление соединений с сервером Zoom, участие в конференциях Zoom, а также обмен сообщениями и файлами при помощи данного приложения.

Примечание: Чтобы позволить приложениям со встроенными SSL-сертификатами подключаться к своим серверам, соответствующие хосты должны быть включены в белый список для протокола SSL (см. Белый список протоколов).

Управлять политиками безопасности для сетевых протоколов можно при помощи консолей управления DeviceLock Management Console, DeviceLock Group Policy Manager или DeviceLock Service Settings Editor. Для просмотра и изменения политик безопасности можно также использовать модуль Отчет о разрешениях/аудите из приложения DeviceLock Enterprise Manager.

Узел “Протоколы”

Узел **Протоколы** позволяет получить доступ к следующим функциям DeviceLock:

- Разрешения для протоколов (см. Разрешения на доступ к протоколам, Управление разрешениями для автономного режима)
- Аудит, теневое копирование и алерты для протоколов (см. Аудит, теневое копирование и алерты для протоколов, Управление правилами аудита, теневого копирования и оповещений для автономного режима)
- Белый список протоколов (см. Белый список протоколов, Управление белым списком протоколов для автономного режима)
- Базовый IP-файрвол (см. Базовый IP-файрвол, Управление базовым IP-файрволом для автономного режима)
- Контентно-зависимые правила для протоколов (см. Правила для протоколов в разделе Контентно-зависимые правила (обычный профиль), а также Управление контентно-зависимыми правилами для протоколов для автономного режима)
- Настройки безопасности для протоколов (см. Настройки безопасности для протоколов, Управление настройками безопасности для автономного режима)

Контекстное меню этого узла **Протоколы** содержит следующие команды:

- **Сбросить политику NetworkLock в неопределенное состояние** - Сбрасывает все настройки NetworkLock в состояние “не задано”.
- **Сбросить политику ContentLock в неопределенное состояние** - Сбрасывает настройки ContentLock (все правила работы с контентом, кроме тех, которые основаны на типах файлов) в состояние “не задано”.

Рекомендации

После настройки разрешений на доступ к протоколам возможна ошибка “Таймаут сервера” при попытке соединения с некоторыми защищенными веб-узлами. Эта проблема вызвана тем, что DeviceLock шифрует трафик SSL, используя свой собственный сертификат, в то время как некоторые веб-сайты и приложения могут работать только с собственным (предопределенным) сертификатом.

Для устранения проблемы необходимо добавить правило белого списка для протокола SSL с указанием доменных имен или IP-адресов и портов, используемых серверами этих веб-сайтов и приложений (инструкции по настройке правил см. в разделе Задание белого списка протоколов).

В случае веб-приложения следует прежде всего определить его серверы подключения. Это можно сделать, например, с помощью инструмента TCP View, который можно скачать по адресу docs.microsoft.com/sysinternals/downloads/tcpview. Некоторые приложения используют пулы серверов с зарезервированными диапазонами IP-адресов, что затрудняет настройку правил белого списка. В этом случае мы рекомендуем обратиться в службу поддержки приложения для получения полного списка используемых IP-адресов (диапазонов).

Разрешения на доступ к протоколам

Чтобы контролировать обмен информацией на транспортном уровне, необходимо настроить применение политик доступа к протоколам, установив соответствующие разрешения. Эти разрешения определяют, какие пользователи будут иметь доступ к указанным протоколам и какой уровень доступа будет при этом предоставляться. Разрешения можно настраивать для пользователей и групп. Описание прав доступа для каждого протокола приводится в разделе Права доступа.

Если в дереве консоли выбран узел **Протоколы** > **Разрешения**, панель сведений отображает список протоколов, для которых можно установить разрешения (см. Действия по управлению разрешениями).

Права доступа

В следующих разделах описываются права доступа, предназначенные для настройки разрешений на доступ к протоколам:

- Поиск работы
- Файловые хранилища
- FTP
- HTTP
- IBM Notes
- ICQ Messenger
- IRC
- Jabber
- Mail.ru Агент
- MAPI
- Skype
- SMB
- SMTP
- Социальные сети
- Telegram
- Telnet
- Торрент
- Viber
- Web-почта
- Web-поиск
- WhatsApp
- Zoom

Поиск работы

Права доступа, применимые к протоколу Поиск работы:

- **Основные: Отправка/Получение данных** - Право на доступ, вход и просмотр сайтов поиска работы.
- **Основные: Поиск** - Право выполнять поиск вакансий на сайтах поиска работы.
- **Основные: Исходящие сообщения** - Право отправлять сообщения, резюме и другие данные через веб-формы на сайтах поиска работы.
- **Основные: Исходящие файлы** - Право загружать файлы на сайты поиска работы.

Файловые хранилища

Права доступа, применимые к протоколу Файловые хранилища:

- **Основные: Отправка/Получение данных** - Право на доступ к файлообменному сайту, просмотр его содержимого и загрузку файлов.
- **Основные: POST-запросы** - Право на отправку данных веб-форм, например комментариев к отдельным файлам. Это право не распространяется на учетные данные, которые вводятся в окне авторизации.
- **Основные: Исходящие файлы** - Право отправлять файлы на сайт обмена файлами.
- **SSL: Отправка/Получение данных** - Право на доступ к сайту обмена файлами, просмотр его содержимого и загрузку файлов по SSL.
- **SSL: POST-запросы** - Право на отправку данных веб-форм по SSL, например комментариев к отдельным файлам. Это право не распространяется на учетные данные, которые вводятся в окне авторизации.
- **SSL: Исходящие файлы** - Право отправлять файлы на файлообменный сайт по SSL.

Примечание: Право POST-запросы для протокола Файловые хранилища, примененное к сервису iCloud, определяет право пользователя на загрузку не-файловых данных (почта, заметки, календарь, контакты, напоминания) в облако iCloud. Аналогичное право используется для включения аудита и теневого копирования не-файловых данных, загружаемых пользователем на iCloud.

FTP

Права доступа, применимые к протоколу FTP:

- **Основные: Отправка/Получение данных** - Право подключаться к FTP-серверу, получать и отправлять служебные данные протокола, загружать файлы с FTP-сервера.
- **Основные: Исходящие файлы** - Право отправлять файлы на FTP-сервер.
- **SSL: Отправка/Получение данных** - Право подключаться к FTP-серверу, получать и отправлять служебные данные протокола, загружать файлы с FTP-сервера, используя FTPS.
- **SSL: Исходящие файлы** - Право отправлять файлы на FTP-сервер, используя FTPS.

HTTP

Права доступа, применимые к протоколу HTTP:

- **Основные: Отправка/Получение данных** - Право подключаться к веб-серверу, получать и отправлять служебные данные протокола, веб-страницы и объекты на веб-страницах (скрипты, Flash-файлы, изображения в формате JPEG, PNG и GIF и т.д.), загружать файлы.
- **Основные: POST-запросы** - Право отправлять данные веб-форм на веб-сервер, используя HTTP.
- **Основные: Исходящие файлы** - Право отправлять файлы на веб-сервер, используя HTTP.
- **SSL: Отправка/Получение данных** - Право подключаться к веб-серверу, получать и отправлять служебные данные протокола, веб-страницы и объекты на веб-страницах (скрипты, Flash-файлы, изображения в формате JPEG, PNG и GIF и т.д.), загружать файлы, используя HTTPS.
- **SSL: POST-запросы** - Право отправлять данные веб-форм на веб-сервер, используя HTTPS.
- **SSL: Исходящие файлы** - Право отправлять файлы на веб-сервер, используя HTTPS.

IBM Notes

Права доступа, применимые к протоколу IBM Notes:

- **Основные: Отправка/Получение данных** - Право подключаться к серверу IBM Domino через клиент IBM Notes и читать почту.
- **Основные: Исходящие сообщения** - Право на отправку почтовых сообщений из клиента IBM Notes на сервер IBM Domino.
- **Основные: Исходящие файлы** - Право на отправку почтовых вложений из клиента IBM Notes на сервер IBM Domino.

ICQ Messenger

Права доступа, применимые к протоколу ICQ Messenger:

- **Основные: Отправка/Получение данных**, **Исходящие сообщения** - Право подключаться к серверу ICQ Messenger, отправлять/получать мгновенные сообщения и получать файлы.
- **Основные: Исходящие файлы** - Право отправлять файлы.
- **SSL: Отправка/Получение данных**, **Исходящие сообщения** - Право подключаться к серверу ICQ Messenger, отправлять/получать мгновенные сообщения и получать файлы по SSL.
- **SSL: Исходящие файлы** - Право отправлять файлы по SSL.

IRC

Права доступа, применимые к протоколу IRC:

- **Основные: Отправка/Получение данных**, **Исходящие сообщения** - Право подключаться к IRC-серверу, отправлять/получать мгновенные сообщения и получать файлы.
- **Основные: Исходящие файлы** - Право отправлять файлы.
- **SSL: Отправка/Получение данных, Исходящие сообщения** - Право подключаться к IRC-серверу, отправлять/получать мгновенные сообщения и получать файлы, используя SSL.
- **SSL: Исходящие файлы** - Право отправлять файлы, используя SSL.

Jabber

Права доступа, применимые к протоколу Jabber:

- **Основные: Отправка/Получение данных**, **Исходящие сообщения** - Право подключаться к серверу Jabber, отправлять/получать мгновенные сообщения и получать файлы.
- **Основные: Исходящие файлы** - Право отправлять файлы.

Mail.ru Агент

Права доступа, применимые к протоколу Mail.ru Агент:

- **Основные: Отправка/Получение данных**, **Исходящие сообщения** - Право подключаться к серверу Mail.ru через Mail.ru Агент, отправлять/получать мгновенные сообщения и получать файлы.
- **Основные: Исходящие файлы** - Право отправлять файлы.

MAPI

Права доступа, применимые к протоколу MAPI:

- **Основные: Отправка/Получение данных** - Право подключаться к серверу Microsoft Exchange через клиентское приложение Outlook и читать почту.
- **Основные: Исходящие сообщения** - Право на отправку почтовых сообщений без вложений из клиентского приложения Outlook на сервер Microsoft Exchange.
- **Основные: Исходящие файлы** - Право на отправку почтовых вложений из клиентского приложения Outlook на сервер Microsoft Exchange.

Примечание: По умолчанию права доступа для протокола MAPI применяются также к папке черновиков, сохраняемых приложением Outlook на сервере Exchange, и к сообщениям, которые импортируются из внешних файлов почтовых сообщений (.msg-файлов) или других (внешних) почтовых ящиков. Это поведение можно изменить, отключив настройку **Перехватывать черновики MAPI-сообщений** и/или **Перехватывать перемещенные MAPI-сообщения** (см. Настройки безопасности для протоколов).

Skype

Права доступа, применимые к протоколу Skype:

- **Основные: Отправка/Получение данных** - Право подключаться к серверу Skype и получать файлы/мгновенные сообщения.
- **Основные: Входящие звонки** - Право принимать звонки.
- **Основные: Исходящие звонки** - Право совершать звонки.
- **Основные: Исходящие сообщения** - Право отправлять мгновенные сообщения.
- **Основные: Исходящие файлы** - Право отправлять файлы.

SMB

Права доступа, применимые к протоколу SMB:

- **Основные: Отправка/Получение данных** - Право подключаться и просматривать содержимое общих сетевых папок на SMB-серверах.
- **Основные: Входящие файлы** - Право скачивать файлы с SMB-серверов на компьютер, на котором работает сервис DeviceLock, а также загружать файлы в общие сетевые папки этого компьютера.
- **Основные: Исходящие файлы** - Право загружать файлы с компьютера, на котором работает сервис DeviceLock, на SMB-серверы, а также скачивать файлы из общих сетевых папок этого компьютера.

Примечание:

- Права доступа для протокола SMB не влияют на процесс регистрации общих сетевых принтеров на компьютерах, контролируемых сервисом DeviceLock. Даже если DeviceLock настроен так, что обмен данными по протоколу SMB блокируется, это не помешает операционной системе загрузить драйвер сетевого принтера. Однако, в данном случае DeviceLock не позволит пользователю загрузить драйвер сетевого принтера вручную.
- Права доступа для протокола SMB не влияют на работу групповой политики на компьютерах в среде Active Directory. Даже если DeviceLock настроен на блокировку обмена данными по протоколу SMB, это не относится к обмену данными групповой политики. Параметры групповой политики обновляются и применяются независимо от прав доступа для протокола SMB.

SMTP

Права доступа, применимые к протоколу SMTP:

- **Основные: Отправка/Получение данных** - Право подключаться к SMTP-серверу, получать и отправлять служебные данные протокола.
- **Основные: Исходящие сообщения** - Право отправлять сообщения электронной почты без вложений.
- **Основные: Исходящие файлы** - Право отправлять вложения электронной почты.
- **SSL: Отправка/Получение данных** - Право подключаться к SMTP-серверу, получать и отправлять служебные данные протокола, используя SSL.
- **SSL: Исходящие сообщения** - Право отправлять сообщения электронной почты без вложений, используя SSL.
- **SSL: Исходящие файлы** - Право отправлять вложения электронной почты, используя SSL.

Социальные сети

Права доступа, применимые к протоколу Социальные сети:

- **Основные: Отправка/Получение данных** - Право на просмотр сайта социальной сети.
- **Основные: Исходящие сообщения** - Право отправлять сообщения, комментарии и т.п.
- **Основные: Исходящие файлы** - Право отправлять медиа-файлы и другие файлы на сайт социальной сети.

Telegram

Права доступа, применимые к протоколу Telegram:

- **Основные: Отправка/Получение данных** - Право использовать Telegram Desktop. Разрешает доступ к серверам Telegram.
- **Основные: Отправка/Получение данных (веб)** - Право использовать Telegram Web. Разрешает доступ к хосту Telegram Web (web.telegram.org).

Telnet

Права доступа, применимые к протоколу Telnet:

- **Основные: Отправка/Получение данных** - Право подключаться к Telnet-серверу, получать и отправлять служебные данные протокола.

Торрент

Права доступа, применимые к протоколу Торрент:

- **Основные: Отправка/Получение данных** - Право подключаться к удаленным хостам по протоколу Торрент.

Viber

Права доступа, применимые к протоколу Viber:

- **Основные: Отправка/Получение данных**, **Исходящие сообщения** - Право подключаться к серверу Viber, отправлять и получать мгновенные сообщения, а также получать файлы.
- **Основные: Исходящие файлы** - Право отправлять файлы.

Web-почта

Права доступа, применимые к протоколу Web-почта:

- **Основные: Отправка/Получение данных** - Право заходить в веб-почту и читать почту.
- **Основные: Исходящие сообщения** - Право отправлять сообщения электронной почты без вложений.
- **Основные: Исходящие файлы** - Право отправлять вложения электронной почты.
- **SSL: Отправка/Получение данных** - Право заходить в веб-почту и читать почту, используя SSL.
- **SSL: Исходящие сообщения** - Право отправлять сообщения электронной почты без вложений, используя SSL.
- **SSL: Исходящие файлы** - Право отправлять вложения электронной почты, используя SSL.

Web-поиск

Права доступа, применимые к протоколу Web-поиск:

- **Основные: Поиск** - Право выполнять поиск в интернете при помощи запросов на сайтах веб-поиска или путем ввода в адресную строку веб-браузера URL-адресов, содержащих поисковые запросы.

WhatsApp

Права доступа, применимые к протоколу WhatsApp:

- **Основные: Отправка/Получение данных** - Право использовать приложение WhatsApp Desktop на компьютерах под управлением Windows.
- **Основные: Отправка/Получение данных (веб)** - Право использовать WhatsApp в веб-браузерах на компьютерах под управлением Windows.

Zoom

Права доступа, применимые к протоколу Zoom:

- **Основные: Отправка/Получение данных** - Право подключаться к серверу Zoom, использовать приложение Zoom для видео- и аудиоконференцсвязи и вебинаров, а также получать сообщения и файлы через это приложение.
- **Основные: Исходящие звонки** - Право участвовать в конференциях Zoom.
- **Основные: Исходящие сообщения** - Право отправлять мгновенные сообщения из приложения Zoom.
- **Основные: Исходящие файлы** - Право отправлять файлы из приложения Zoom.

Разрешения по умолчанию

В диалоговом окне **Разрешения** предоставляется возможность установить разрешения по умолчанию для доступа к протоколам. Эти разрешения назначаются группам Администраторы (Administrators) и Все (Everyone), а также учетной записи СИСТЕМА (SYSTEM) в случае протокола SMB. В следующей таблице перечислены разрешения по умолчанию для каждого протокола.

Учетная запись/ Протокол	**Администраторы**	**Все**
Поиск работы	Основные: Отправка/Получение данных, Поиск, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Поиск, Исходящие сообщения
Файловые хранилища	Основные: Отправка/Получение данных, POST-запросы, Исходящие файлы SSL: Отправка/Получение данных, POST-запросы, Исходящие файлы	Основные: Отправка/Получение данных, POST-запросы SSL: Отправка/Получение данных, POST-запросы
FTP	Основные: Отправка/Получение данных, Исходящие файлы SSL: Отправка/Получение данных, Исходящие файлы	Основные: Отправка/Получение данных SSL: Отправка/Получение данных
HTTP	Основные: Отправка/Получение данных, POST-запросы, Исходящие файлы SSL: Отправка/Получение данных, POST-запросы, Исходящие файлы	Основные: Отправка/Получение данных, POST-запросы SSL: Отправка/Получение данных, POST-запросы
IBM Notes	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения
ICQ Messenger	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы SSL: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения SSL: Отправка/Получение данных, Исходящие сообщения
IRC	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы SSL: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения SSL: Отправка/Получение данных, Исходящие сообщения
Jabber	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения
Mail.ru Агент	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения
MAPI	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения

Учетная запись/ Протокол	Администраторы	Все
Skype	Основные: Отправка/Получение данных, Входящие звонки, Исходящие сообщения, Исходящие файлы, Исходящие звонки	Основные: Отправка/Получение данных, Входящие звонки, Исходящие сообщения, Исходящие звонки
SMB	Основные: Отправка/Получение данных, Входящие файлы, Исходящие файлы **Примечание:** В случае протокола SMB эти разрешения по умолчанию назначаются также учетной записи СИСТЕМА.	Основные: Отправка/Получение данных
SMTP	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы SSL: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения SSL: Отправка/Получение данных, Исходящие сообщения
Социальные сети	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения
Telegram	Основные: Отправка/Получение данных, Отправка/Получение данных (веб)	Основные: Отправка/Получение данных, Отправка/Получение данных (веб)
Telnet	Основные: Отправка/Получение данных	Основные: Отправка/Получение данных
Торрент	Основные: Отправка/Получение данных	Основные: Отправка/Получение данных
Viber	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения
Web-почта	Основные: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы SSL: Отправка/Получение данных, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие сообщения SSL: Отправка/Получение данных, Исходящие сообщения
Web-поиск	Основные: Поиск	Основные: Поиск
WhatsApp	Основные: Отправка/Получение данных, Отправка/Получение данных (веб)	Основные: Отправка/Получение данных, Отправка/Получение данных (веб)
Zoom	Основные: Отправка/Получение данных, Исходящие звонки, Исходящие сообщения, Исходящие файлы	Основные: Отправка/Получение данных, Исходящие звонки, Исходящие сообщения

Действия по управлению разрешениями

Управление разрешениями для протоколов для оперативного режима предполагает:

- Задание и редактирование разрешений
- Сброс разрешений в исходное состояние

Примечание: Можно установить разрешения на доступ к протоколам для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Разрешения для оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Разрешения для автономного режима (офлайн-профиль) применяются, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Для получения дополнительной информации о политиках DeviceLock для автономного режима работы см. раздел Политики безопасности DeviceLock (офлайн-профиль). Для получения информации о том, как установить разрешения для автономного режима, см. раздел Управление разрешениями для автономного режима.

Разрешения для оперативного режима могут иметь одно из следующих состояний:

- **Задано** - Разным учетным записям назначены разные разрешения для данного протокола.
- **Полный доступ** - У всех учетных записей есть полный доступ к данному протоколу.

  Это состояние отображается, например, когда разрешения заданы только для учетной записи Все (Everyone) таким образом, что у нее есть полный доступ к протоколу.
- **Нет доступа** - Нет учетных записей, имеющих доступ к данному протоколу.

  Это состояние отображается, например, когда учетной записи Все (Everyone) явно запрещен любой доступ к данному протоколу или разрешения не заданы ни для каких учетных записей. Обратите внимание, что запрет для учетной записи Все (Everyone) отменяет любые разрешения для других учетных записей.
- **Не задано** - Настройки разрешений для данного протокола не заданы.

Задание и редактирование разрешений

Чтобы задать и редактировать разрешения

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выберите **Разрешения**.

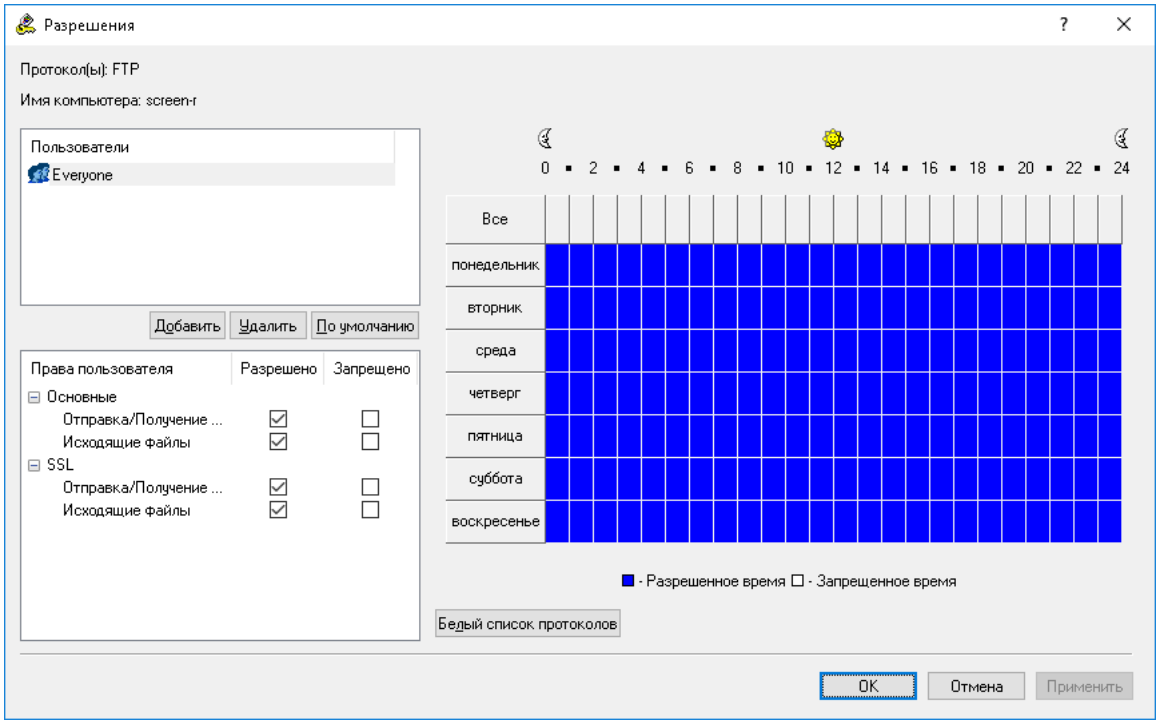
   Если в дереве консоли выбрать "Разрешения", на панели сведений отобразятся протоколы, для которых можно установить разрешения. На панели сведений в столбце "Обычный" также отображается текущее состояние разрешений на каждый протокол для оперативного режима.
4. На панели сведений выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши протокол, для которого требуется установить или редактировать разрешения, а затем выберите команду **Установить разрешения**.

     - или -
   - Выберите протокол, для которого требуется установить или редактировать разрешения, а затем щелкните значок **Установить разрешения** на панели инструментов.

   Чтобы выбрать одновременно несколько протоколов, используйте клавиши SHIFT или CTRL.

   Примечание: При выборе нескольких протоколов, имеющих разные наборы возможных прав доступа, необходимо учесть следующее:
   - Диалоговое окно **Разрешения** отображает только те права доступа, которые являются общими для всех выбранных протоколов. Разрешая или запрещая какие-либо из отображаемых прав доступа, вы настраиваете доступ к каждому из выбранных протоколов.
   - Некоторые права доступа зависят от других прав. Если предоставляется право, зависящее от другого права, необходимое право предоставляется автоматически. Например, если для социальных сетей и веб-почты предоставить только право **Основные: Исходящие файлы**, автоматически будут предоставлены следующие права: **Основные: Отправка/Получение данных**, **Основные: Исходящие сообщения**.

Появится диалоговое окно “Разрешения”.



5. В диалоговом окне **Разрешения** выполните следующие действия:

Чтобы установить разрешения по умолчанию

- В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **По умолчанию**.

  По умолчанию разрешения устанавливаются для групп Администраторы (Administrators) и Все (Everyone). Подробнее см. в разделе Разрешения по умолчанию ранее в этом документе.

Чтобы настроить разрешения для нового пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

b) В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой верхней части диалогового окна “Разрешения”.

c) В левой верхней части диалогового окна **Разрешения** в области **Пользователи** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

d) На левой нижней панели диалогового окна **Разрешения** в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права (см. Права доступа).

В правой части диалогового окна "Разрешения" можно указать дни недели и время, когда будет предоставлен доступ к выбранным протоколам. Используйте левую кнопку мыши, чтобы выбрать дни недели и время, когда выбранному пользователю или группе будет предоставлен доступ к выбранным протоколам. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда доступ будет запрещен.

Чтобы изменить разрешения для имеющегося пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу.

b) На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

Чтобы удалить имеющегося пользователя или группу и разрешения

- В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или клавишу DELETE.

Чтобы задать, просмотреть или изменить правила белого списка для данного протокола

- Нажмите кнопку **Белый список протоколов**. Подробнее о белом списке см. в разделе Белый список протоколов.

Чтобы задать, просмотреть или изменить настройки безопасности для протокола MAPI

- Нажмите кнопку **Настройки безопасности**. Подробнее о настройках безопасности см. в разделе Настройки безопасности для протоколов.

Примечание: Кнопка **Настройки безопасности** появляется в диалоговом окне **Разрешения** только при управлении разрешениями для протокола MAPI. Для других протоколов эта кнопка отсутствует.

6. Нажмите кнопку **OK** или **Применить**.

Сброс разрешений в исходное состояние

Возврат разрешений в исходное “неопределенное” состояние. Если для развертывания политик DeviceLock используется DeviceLock Group Policy Manager или DeviceLock Service Settings Editor, могут возникнуть ситуации, когда потребуется отменить применение заданных разрешений к определенной группе компьютеров. Для этого необходимо вернуть ранее заданные разрешения в исходное “неопределенное” состояние. Все параметры DeviceLock, которые установлены в состояние “не определен”, игнорируются на клиентских компьютерах.

Чтобы сбросить разрешения в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.
   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выберите **Разрешения**.

   Если в дереве консоли выбрать “Разрешения”, на панели сведений отобразится список протоколов, для которых можно установить разрешения.
4. На панели сведений щелкните правой кнопкой мыши протокол, для которого требуется вернуть разрешения в исходное “неопределенное” состояние, а затем выберите команду **Сбросить**.

   Можно вернуть разрешения в исходное “неопределенное” состояние для нескольких протоколов одновременно. Чтобы это сделать, выполните следующее:
   a) На панели сведений выберите несколько протоколов, удерживая клавишу SHIFT или CTRL и щелкая протоколы.
   b) Щелкните правой кнопкой мыши выбранные протоколы, и выберите команду **Сбросить**.

Аудит, теневое копирование и алерты для протоколов

DeviceLock позволяет выполнять аудит доступа и теневое копирование файлов и данных, передаваемых по сетевым каналам. Аудит и теневое копирование позволяют отслеживать и записывать критически важные для безопасности события, связанные с передачей данных по сети. Регулярный анализ журналов аудита является эффективным способом выявления утечек данных и расследования инцидентов безопасности, вызванных потерей или кражей данных.

Если в дереве консоли выбран узел **Протоколы** > **Аудит, Теневое Копирование и Алерты**, панель сведений отображает список протоколов, для которых можно установить правила аудита и теневого копирование (см. Действия по управлению аудитом, теневым копированием и алертами). Используя этот узел, можно также включить алерты (тревожные оповещения), которые будут рассылаться при попытке пользователя обратиться к протоколу определенного типа (см. Включение тревожных оповещений).

Для записи данных аудита и теневого копирования DeviceLock использует два типа журналов: журнал аудита и журнал теневого копирования. Журнал аудита используется для отслеживания действий пользователей и записи событий доступа к протоколам. Данные аудита могут быть записаны в стандартную подсистему ведения протоколов событий (журнал событий Windows), в собственный журнал DeviceLock или одновременно в оба журнала. Возможна также отправка данных на сервер syslog. Чтобы указать, куда следует сохранять данные аудита, используйте параметр Тип журнала аудита из списка Настройки сервиса. Для просмотра данных аудита используйте просмотрщики журнала аудита (см. Просмотрщик журнала аудита (для компьютера) и Просмотрщик журнала аудита (для сервера)).

Журнал теневого копирования используется для хранения полных копий файлов и данных, передаваемых по сетевым каналам. Для просмотра данных теневого копирования используйте просмотрщики журнала теневого копирования (см. Просмотрщик журнала теневого копирования (для компьютера) и Просмотрщик журнала теневого копирования (для сервера)).

Чтобы включить аудит и теневое копирование данных, передаваемых через указанные протоколы, необходимо задать правила аудита и теневого копирования. В каждом правиле для протокола задаются пользователи и группы, к которым применяется это правило, а также соответствующие права аудита и теневого копирования, которые определяют, для каких действий пользователя выполнять аудит и теневое копирование.

События аудита предоставляют различную информацию, такую как тип события, дата и время события, используемый протокол, имя пользователя, связанного с событием, информация о процессе и другая информация, специфичная для конкретного типа события.

Примечание: При использовании теневого копирования необходимо учитывать следующее:

- Если передача данных запрещена на уровне типа (разрешения для протоколов), то теневая копия передаваемых данных не будет создана, так как в этом случае DeviceLock блокирует передачу данных до начала их перехвата. Исключение: Если данные проверяются контентно-зависимыми правилами, то DeviceLock создает теневую копию данных, даже если их передача запрещена на уровне типа.

Права аудита и теневого копирования

В следующих разделах описываются права аудита и теневого копирования, используемые при создании правил, а также дается специфичная для типа события информация, записываемая в журнал:

- Поиск работы
- Файловые хранилища
- FTP
- HTTP
- IBM Notes
- ICQ Messenger
- IRC
- Jabber
- Mail.ru Агент
- MAPI
- Skype
- SMB
- SMTP
- Социальные сети
- Telegram
- Telnet
- Торрент
- Viber
- Web-почта
- Web-поиск
- WhatsApp
- Zoom

Поиск работы

Права аудита и теневого копирования, применимые к протоколу Поиск работы:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с сайтом поиска работы.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя веб-узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Поиск** - Включает аудит попыток пользователя подать запрос на поиск вакансий на сайте поиска работы.

  В журнал аудита записывается событие "Поиск", имя службы поиска работы, введенная пользователем строка поиска, IP-адрес, номер порта и имя веб-узла, а также имя протокола.

- **Аудит: Исходящие сообщения** - Включает аудит попыток пользователя отправить сообщение, резюме или другие данные через веб-форму на сайте поиска работы.

  В журнал аудита записывается событие "Исходящее сообщение", а также сведения для идентификации отправленного контента в следующем формате: <имя_сайта>: <название_контента>. Идентификатор получателя записывается только в случае отправки сообщений.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя загрузить файл на сайт поиска работы.

  В журнал аудита записывается событие "Исходящий файл", а также сведения для идентификации загруженного файла (<имя_сайта>: <имя_файла>).

- **Теневое копирование: Поиск** - Включает теневое копирование введенных пользователем запросов на поиск вакансий на сайтах поиска работы.

  В журнал теневого копирования записывается копия каждого поискового запроса.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование сообщений, резюме и других данных, отправленных через веб-формы на сайтах поиска работы.

  В журнал теневого копирования записываются копии сообщений, резюме и других данных, отправленных через веб-формы.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование файлов, загруженных на сайты поиска работы.

  В журнал теневого копирования записываются копии загруженных файлов.

Файловые хранилища

Права аудита и теневого копирования, применимые к протоколу Файловые хранилища:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с файлообменным сайтом.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя веб-узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя загрузить файл с файлообменного сайта.

  В журнал аудита записывается событие "Входящий файл", IP-адрес, номер порта и имя узла, а также имя протокола.

- **Аудит: POST-запросы** - Включает аудит попыток пользователя отправить данные веб-форм, например комментарии к отдельным файлам.

  В журнал аудита записывается событие "POST-запрос", имя службы хранения файлов, общего доступа или синхронизации, IP-адрес, номер порта и имя узла, а также имя протокола.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл на файлообменный сайт.

  В журнал аудита записывается событие "Исходящий файл", имя файла, IP-адрес, номер порта и имя узла, а также имя протокола.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование файлов, скачанных с файлообменного сайта.

  В журнал теневого копирования записываются копии скачанных файлов.

- **Теневое копирование: POST-запросы** - Включает теневое копирование отправленных данных веб-форм (комментарии к отдельным файлам).

  В журнал теневого копирования записываются копии отправленных данных веб-форм.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование файлов, загруженных на файлообменный сайт.

  В журнал теневого копирования записываются копии загруженных файлов.

Примечание: Право POST-запросы для протокола Файловые хранилища, примененное к сервису iCloud, разрешает аудит и теневое копирование не-файловых данных (почта, заметки, календарь, контакты, напоминания). В записях аудита и теневых копиях этих данные идентифицируются как исходящие сообщения.

FTP

Права аудита и теневого копирования, применимые к протоколу FTP:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с FTP-сайтом.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя ftp-узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя загрузить файл с FTP-сайта.

  В журнал аудита записывается событие "Входящий файл", абсолютный путь к файлу и его полное имя (например, ftp://myftp/myfile.doc), IP-адрес, номер порта и имя узла.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл на FTP-сайт.

  В журнал аудита записывается событие "Исходящий файл", абсолютный путь к файлу и его полное имя (например, ftp://myftp/myfile.doc), IP-адрес, номер порта и имя узла.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование файлов, скачанных с FTP-сайта.

  В журнал теневого копирования записываются копии скачанных файлов.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование файлов, загруженных на FTP-сайт.

  В журнал теневого копирования записываются копии загруженных файлов.

HTTP

Права аудита и теневого копирования, применимые к протоколу HTTP:

- **Аудит: Соединение** - Включает аудит для разрешенных и заблокированных попыток пользователя открыть веб-страницу.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя веб-узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

  Примечание: Если это право включено, при попытке пользователя открыть веб-страницу в журнал аудита записывается множество событий "Соединение". Такое поведение вызвано тем, что веб-страницы зачастую содержат ссылки на ресурсы (изображения, скрипты и т.п.), расположенные на других веб-узлах.

- **Аудит: Входящие данные** - Включает аудит веб-страниц и их объектов.

  В журнал аудита записывается событие "Входящие данные", URL-адрес веб-страницы и объектов на веб-странице (например, абсолютный путь с указанием URL до параметров запроса http://domain/path), IP-адрес, номер порта и имя узла.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя загрузить файл с веб-сайта.

  В журнал аудита записывается событие "Входящий файл", абсолютный путь к файлу и его полное имя (например, http://domain/path/myfile.doc), IP-адрес, номер порта и имя узла.

- **Аудит: Исходящие данные** - Тип данных "Исходящие данные" не содержит данных.

  В журнал аудита записывается событие "Исходящие данные", URL-адрес веб-страницы и объектов на веб-странице (например, абсолютный путь с указанием URL до параметров запроса http://domain/path), IP-адрес, номер порта и имя узла.

- **Аудит: POST-запросы** - Включает аудит попыток пользователя отправить данные веб-форм на веб-сайт.

  В журнал аудита записывается событие "POST-запрос" и URL-адрес скрипта, отправившего POST-запрос (например, абсолютный путь с указанием URL до параметров запроса http://domain/path).

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл на веб-сайт.

  В журнал аудита записывается событие "Исходящий файл", имя файла и имя сервера-получателя файла (например, http://server/file.doc), IP-адрес, номер порта и имя узла.

- **Теневое копирование: Входящие данные** - Включает теневое копирование веб-страниц и их объектов.

  В журнал теневого копирования записываются копии веб-страниц и их составных частей.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование файлов, скачанных с веб-сайта.

  В журнал теневого копирования записываются копии скачанных файлов.

- **Теневое копирование: Исходящие данные** - Это право не влияет на теневое копирование.
- **Теневое копирование: POST-запросы** - Включает теневое копирование отправленных данных веб-форм.

  В журнал теневого копирования записываются копии отправленных данных веб-форм.
- **Теневое копирование: Исходящие файлы** - Включает теневое копирование файлов, загруженных на веб-сайт.

  В журнал теневого копирования записываются копии загруженных файлов.

IBM Notes

Права аудита и теневого копирования, применимые к протоколу IBM Notes:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с сервером IBM Domino с помощью клиента IBM Notes.

  В журнал аудита записывается событие "Соединение" и IP-адрес или имя узла. При успешном подключении к серверу IBM Domino создается несколько событий "Соединение".
- **Аудит: Входящие сообщения, Входящие файлы** - Включает аудит попыток пользователя получить с сервера IBM Domino через клиент IBM Notes почтовое сообщение с вложениями или без них.

  В журнал аудита записывается событие "Входящее сообщение", количество вложений, адрес электронной почты отправителя и адресатов и тема сообщения. Адрес отправителя предшествует адресам получателей (отправитель => получатель 1, получатель 2).
- **Аудит: Исходящие сообщения, Исходящие файлы** - Включает аудит попыток пользователя отправить почтовое сообщение с вложениями или без них на сервер IBM Domino через клиент IBM Notes.

  В журнал аудита записывается событие "Исходящее сообщение", количество вложений, почтовый адрес отправителя и адресатов и тема сообщения. Адрес отправителя предшествует адресам получателей (отправитель => получатель 1, получатель 2).

  Количество вложений всегда записывается в журнал аудита.
- **Теневое копирование: Входящие сообщения, Входящие файлы** - Включает теневое копирование полученных сообщений электронной почты с вложениями или без них.

  Копии полученных сообщений электронной почты с вложениями или без вложений записываются в журнал теневого копирования в виде EML-файлов. Такие файлы можно открыть, например, в Microsoft Outlook Express, Windows Mail или Mozilla Thunderbird.
- **Теневое копирование: Исходящие сообщения, Исходящие файлы** - Включает теневое копирование отправленных сообщений электронной почты с вложениями или без них.

  Копии отправленных сообщений электронной почты с вложениями или без вложений записываются в журнал теневого копирования в виде EML-файлов. Такие файлы можно открыть, например, в Microsoft Outlook Express, Windows Mail или Mozilla Thunderbird.

  Количество вложений всегда записывается в журнал теневого копирования.

ICQ Messenger

Права аудита и теневого копирования, применимые к протоколу ICQ Messenger:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с сервером ICQ Messenger.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Входящие сообщения, Исходящие сообщения** - Включает аудит попыток пользователя отправить и получить мгновенные сообщения.

  В журнал аудита записывается событие "Чат", идентификаторы (ID) всех участников разговора, IP-адрес, номер порта и имя узла. Идентификатор локального участника разговора предшествует идентификатору удаленного участника разговора.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл", а также имя файла.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл", а также имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных сообщений.

  Копии полученных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из программы обмена сообщениями. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных сообщений.

  Копии отправленных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из программы обмена сообщениями. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

IRC

Права аудита и теневого копирования, применимые к протоколу IRC:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с IRC-сервером.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Входящие сообщения, Исходящие сообщения** - Включает аудит попыток пользователя отправить и получить мгновенные сообщения.

  В журнал аудита записывается событие "Чат", идентификаторы (ID) всех участников разговора, IP-адрес, номер порта и имя узла. Идентификатор локального участника разговора предшествует идентификатору удаленного участника разговора.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл" и имя файла.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл" и имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных сообщений.

  Копии полученных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из программы обмена сообщениями. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных сообщений.

  Копии отправленных мгновенных сообщений записываются в журнал теневого копирование в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из программы обмена сообщениями. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

Jabber

Права аудита и теневого копирования, применимые к протоколу Jabber:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с Jabber-сервером.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Входящие сообщения, Исходящие сообщения** - Включает аудит попыток пользователя отправить и получить мгновенные сообщения.

  В журнал аудита записывается событие "Чат", идентификаторы (ID) всех участников разговора, IP-адрес, номер порта и имя узла. Идентификатор локального участника разговора предшествует идентификатору удаленного участника разговора.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл" и имя файла.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл" и имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных сообщений.

  Копии полученных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из программы обмена сообщениями. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных сообщений.

  Копии отправленных мгновенных сообщений записываются в журнал теневого копирование в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из программы обмена сообщениями. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

Mail.ru Агент

Права аудита и теневого копирования, применимые к протоколу Mail.ru Агент:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение Mail.ru Агент с сервером Mail.ru.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Входящие сообщения, Исходящие сообщения** - Включает аудит попыток пользователя отправить и получить мгновенные сообщения.

  В журнал аудита записывается событие "Чат", идентификаторы (ID) всех участников разговора, IP-адрес, номер порта и имя узла. Идентификатор локального участника разговора предшествует идентификатору удаленного участника разговора.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл" и имя файла.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл" и имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных сообщений.

  Копии полученных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из программы обмена сообщениями. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных сообщений.

  Копии отправленных мгновенных сообщений записываются в журнал теневого копирование в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из программы обмена сообщениями. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

MAPI

Права аудита и теневого копирования, применимые к протоколу MAPI:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с Microsoft Exchange Server с помощью клиента Outlook.

  В журнал аудита записывается событие "Соединение" и IP-адрес или имя узла. При успешном подключении к Microsoft Exchange Server создается несколько событий "Соединение".

- **Аудит: Входящие сообщения, Входящие файлы** - Включает аудит попыток пользователя получить из Microsoft Exchange Server через клиент Outlook почтовое сообщение с вложениями или без них.

  В журнал аудита записывается событие "Входящее сообщение", количество вложений, адрес электронной почты отправителя и адресатов и тема сообщения. Адрес отправителя предшествует адресам получателей (отправитель => получатель 1, получатель 2).

- **Аудит: Исходящие сообщения**, **Исходящие файлы** - Включает аудит попыток пользователя отправить почтовое сообщение с вложениями или без них в Microsoft Exchange Server через клиент Outlook.

  В журнал аудита записывается событие "Исходящее сообщение", количество вложений, почтовый адрес отправителя и адресатов и тема сообщения. Адрес отправителя предшествует адресам получателей (отправитель => получатель 1, получатель 2).

  Количество вложений всегда записывается в журнал аудита.

- **Теневое копирование: Входящие сообщения, Входящие файлы** - Включает теневое копирование полученных сообщений электронной почты с вложениями или без них.

  Копии полученных сообщений электронной почты с вложениями или без вложений записываются в журнал теневого копирования в виде EML-файлов. Такие файлы можно открыть, например, в Microsoft Outlook Express, Windows Mail или Mozilla Thunderbird.

- **Теневое копирование: Исходящие сообщения, Исходящие файлы** - Включает теневое копирование отправленных сообщений электронной почты с вложениями или без них.

  Копии отправленных сообщений электронной почты с вложениями или без вложений записываются в журнал теневого копирования в виде EML-файлов. Такие файлы можно открыть, например, в Microsoft Outlook Express, Windows Mail или Mozilla Thunderbird.

  Количество вложений всегда записывается в журнал теневого копирования.

Примечание:

- При попытке открыть EML-файл из журнала теневого копирования может оказаться, что такой файл невозможно открыть в Outlook 2007. Решение этой проблемы приведено в статье Microsoft по адресу support.microsoft.com/kb/956693.
- Права аудита и теневого копирования для протокола **MAPI** также применяются к черновикам сообщений, не отправленных из приложения Outlook на Exchange Server. Так, если пользователь Outlook имеет право отправлять сообщения, DeviceLock будет регистрировать событие аудита и/или создавать теневую копию для сохраненного черновика сообщения, когда пользователь закрывает Outlook, не отправив сообщение. Если у пользователя нет права на отправку сообщений, событие аудита и/или теневая копия будут создаваться при сохранении черновика сообщения в Outlook.

Skype

Права аудита и теневого копирования, применимые к протоколу Skype:

- **Аудит: Соединение** - Включает аудит попыток пользователя войти в учетную запись Skype.

  В журнал аудита записывается событие "Соединение".

- **Аудит: Входящие звонки** - Включает аудит попыток пользователя принять звонок.

  В журнал аудита записывается событие "Входящий звонок" и имена учетных записей Skype всех участников разговора. Имя Skype локального участника предшествует именам Skype удаленных участников.

- **Аудит: Входящие сообщения** - Включает аудит попыток пользователя получить мгновенное сообщение.

  В журнал аудита записывается событие "Чат" и имена учетных записей Skype всех участников чата. Имя Skype локального участника предшествует именам Skype удаленных участников.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл" и имя файла.

- **Аудит: Исходящие звонки** - Включает аудит попыток пользователя совершить звонок.

  В журнал аудита записывается событие "Исходящий звонок" и имена учетных записей Skype всех участников разговора. Имя Skype локального участника предшествует именам Skype удаленных участников.

- **Аудит: Исходящие сообщения** - Включает аудит попыток пользователя отправить мгновенное сообщение.

  В журнал аудита записывается событие "Чат" и имена учетных записей Skype всех участников чата.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл" и имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных сообщений.

  Копии полученных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из Skype. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных сообщений.

  Копии отправленных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из Skype. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

SMB

Права аудита и теневого копирования, применимые к протоколу SMB:

- **Аудит: Соединение** - Включает аудит попыток пользователя получить доступ к какому-либо SMB-серверу. Также включает аудит попыток других компьютеров получить доступ к общим сетевым папкам компьютера, на котором работает сервис DeviceLock.

  В журнал аудита записывается событие "Соединение", а также имя или IP-адрес SMB-сервера, к которому был запрошен доступ, либо имя или IP-адрес компьютера, запросившего доступ к компьютеру, на котором работает сервис DeviceLock. Чтобы предотвратить загромождение журнала чрезмерным количеством записей о соединениях, регистрируется только первое соединение с данным SMB-сервером или внешним компьютером.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя скачать файлы с какого-либо SMB-сервера. Также включает аудит попыток других компьютеров загрузить файлы в общие сетевые папки компьютера, на котором работает сервис DeviceLock.

  В журнал аудита записывается событие "Входящий файл" и имя каждого входящего файла.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя загрузить файлы на какой-либо SMB-сервер. Также включает аудит попыток других компьютеров скачать файлы из общих сетевых папок компьютера, на котором работает сервис DeviceLock.

  В журнал аудита записывается событие "Исходящий файл" и имя каждого исходящего файла.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование файлов, скачанных с SMB-серверов. Также включает теневое копирование файлов, загруженных другими компьютерами в общие сетевые папки компьютера, на котором работает сервис DeviceLock.

  В журнал теневого копирования записывается копия каждого входящего файла.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование файлов, загруженных на SMB-серверы. Также включает теневое копирование файлов, скачанных другими компьютерами из общих сетевых папок компьютера, на котором работает сервис DeviceLock.

  В журнал теневого копирования записывается копия каждого исходящего файла.

SMTP

Права аудита и теневого копирования, применимые к протоколу SMTP:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с SMTP-сервером.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Исходящие сообщения**, **Исходящие файлы** - Включает аудит попыток пользователя отправить сообщение электронной почты с вложениями или без вложений.

  В журнал аудита записывается событие "Исходящее сообщение", количество вложений, адрес электронной почты отправителя и получателей и тема сообщения. Адрес отправителя предшествует адресам получателей (отправитель => получатель 1, получатель 2).

  Количество вложений всегда записывается в журнал аудита.

- **Теневое копирование: Исходящие сообщения**, **Исходящие файлы** - Включает теневое копирование отправленных сообщений электронной почты с вложениями или без них.

  Копии отправленных сообщений электронной почты с вложениями или без вложений записываются в журнал теневого копирования в виде EML-файлов. Такие файлы можно открыть, например, в Microsoft Outlook Express, Windows Mail или Mozilla Thunderbird.

  Количество вложений всегда записывается в журнал теневого копирования.

Социальные сети

Права аудита и теневого копирования, применимые к протоколу Социальные сети:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с сайтом социальной сети.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя веб-узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Исходящие сообщения** - Включает аудит попыток пользователя отправить сообщения, комментарии и т.п.

  В журнал аудита записывается событие "Исходящее сообщение", а также сведения для идентификации отправленного контента (<имя_сайта>: <название_контента>_<идентификатор_получателя>). Идентификаторы получателей (в числовом формате) записываются в журнал только в случае отправки сообщений.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя загрузить медиа-файлы и другие файлы на сайт социальной сети.

  В журнал аудита записывается событие "Исходящий файл", а также сведения для идентификации загруженного файла (<имя_сайта>: <имя_файла>).

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных сообщений, комментариев и т.п.

  В журнал теневого копирования записываются копии отправленных сообщений, комментариев и т.п.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование файлов, загруженных на сайт социальной сети.

  В журнал теневого копирования записываются копии загруженных файлов.

Telegram

Права аудита и теневого копирования, применимые к протоколу Telegram:

- **Аудит: Соединение** - Включает аудит попыток соединения Telegram Desktop с сервером Telegram.

  В журнал аудита записывается событие "Соединение".

- **Аудит: Соединение (веб)** - Включает аудит попыток соединения с веб-узлом Telegram Web.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу. Чтобы отличить соединение Telegram Web от других соединений Telegram, в поле "Имя" записи о таком соединении указывается слово Web.

- **Аудит: Входящие звонки** - Включает аудит попыток пользователя принять звонок.

  В журнал аудита записывается событие "Входящий звонок" и ID пользователя Telegram каждого участника разговора. ID локального участника предшествует ID удаленных участников.

- **Аудит: Входящие сообщения** - Включает аудит попыток пользователя получить мгновенное сообщение. Может быть выбрано только вместе с правом **Аудит: Исходящие сообщения**.

  В журнал аудита записывается событие "Чат" и ID пользователя Telegram каждого участника чата. ID локального участника предшествует ID удаленных участников.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл" и имя файла.

- **Аудит: Исходящие звонки** - Включает аудит попыток пользователя совершить звонок.

  В журнал аудита записывается событие "Исходящий звонок" и ID пользователя Telegram каждого участника разговора. ID локального участника предшествует ID удаленных участников.

- **Аудит: Исходящие сообщения** - Включает аудит попыток пользователя отправить мгновенное сообщение. Может быть выбрано только вместе с правом **Аудит: Входящие сообщения**.

  В журнал аудита записывается событие "Чат" и ID пользователя Telegram каждого участника чата.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл" и имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных сообщений.

  Копии полученных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из Telegram. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных сообщений.

  Копии отправленных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из Telegram. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

Telnet

Права аудита и теневого копирования, применимые к протоколу Telnet:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с Telnet-сайтом.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

Торрент

Права аудита и теневого копирования, применимые к протоколу Торрент:

- **Аудит: Соединение** - Включает аудит попыток пользователя установить соединение с удаленным узлом по протоколу Торрент.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

Viber

Права аудита и теневого копирования, применимые к протоколу Viber:

- **Аудит: Соединение** - Включает аудит попыток пользователя войти в учетную запись Viber.

  В журнал аудита записывается событие "Соединение".

- **Аудит: Входящие звонки** - Включает аудит попыток пользователя принять звонок.

  В журнал аудита записывается событие "Входящий звонок" и ID пользователя Viber каждого участника разговора. ID локального участника предшествует ID удаленных участников.

- **Аудит: Входящие сообщения** - Включает аудит попыток пользователя получить мгновенное сообщение.

  В журнал аудита записывается событие "Чат" и ID пользователя Viber каждого участника чата. ID локального участника предшествует ID удаленных участников.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл" и имя файла.

- **Аудит: Исходящие звонки** - Включает аудит попыток пользователя совершить звонок.

  В журнал аудита записывается событие "Исходящий звонок" и ID пользователя Viber каждого участника разговора. ID локального участника предшествует ID удаленных участников.

- **Аудит: Исходящие сообщения** - Включает аудит попыток пользователя отправить мгновенное сообщение.

  В журнал аудита записывается событие "Чат" и ID пользователя Viber каждого участника чата. ID локального участника предшествует ID удаленных участников.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл" и имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных сообщений.

  Копии полученных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из Viber. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных сообщений.

  Копии отправленных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из Viber. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

Web-почта

Права аудита и теневого копирования, применимые к протоколу Web-почта:

- **Аудит: Соединение** - Включает аудит попыток пользователя получить доступ к веб-почте.

  В журнал аудита записывается событие "Соединение", IP-адрес, номер порта и имя веб-узла, а также имя протокола. Имя узла не приводится, если его не удалось определить по IP-адресу.

- **Аудит: Исходящие сообщения, Исходящие файлы** - Включает аудит попыток пользователя отправить сообщение электронной почты с вложениями или без вложений.

  В журнал аудита записывается событие "Исходящее сообщение", имя почтовой веб-службы (Yahoo, Gmail, Hotmail и т.д.), количество вложений, адрес электронной почты отправителя и получателей и тема сообщения. Адрес отправителя предшествует адресам получателей (отправитель => получатель 1, получатель 2).

  Количество вложений всегда записывается в журнал аудита.

- **Теневое копирование: Исходящие сообщения**, **Исходящие файлы** - Включает теневое копирование отправленных сообщений электронной почты с вложениями или без них.

  Копии отправленных сообщений электронной почты с вложениями или без вложений записываются в журнал теневого копирования в виде EML-файлов. Такие файлы можно открыть, например, в Microsoft Outlook Express, Windows Mail или Mozilla Thunderbird.

  Количество вложений всегда записывается в журнал теневого копирования.

Примечание: Почтовые службы автоматически сохраняют черновики сообщений. DeviceLock обрабатывает сохранение черновика так же, как отправку сообщения.

Web-поиск

Права аудита и теневого копирования, применимые к протоколу Web-поиск:

- **Аудит: Поиск** - Включает аудит попыток пользователя отправить запрос на сайте веб-поиска или ввести в адресную строку веб-браузера URL-адрес, в котором содержится поисковый запрос.

  В журнал аудита записывается событие "Поиск", имя службы веб-поиска, введенная пользователем строка поиска, IP-адрес, номер порта и имя веб-узла, а также имя протокола.

- **Теневое копирование: Поиск** - Включает теневое копирование поисковых запросов, введенных пользователем.

  В журнал теневого копирования записывается копия каждого поискового запроса.

WhatsApp

Права аудита и теневого копирования, применимые к протоколу WhatsApp:

- **Аудит: Соединение** - Включает аудит попыток приложения WhatsApp Desktop подключиться к серверу WhatsApp.

  В журнал аудита записывается событие "Соединение".

- **Аудит: Соединение (веб)** - Включает аудит попыток соединения с веб-узлом WhatsApp Web.

  В журнал аудита записывается событие "Соединение". В отличие от соединений WhatsApp Desktop, в поле "Имя" записи о соединении с веб-узлом WhatsApp Web указывается слово Web.

- **Аудит: Входящие сообщения** - Включает аудит попыток пользователя получить мгновенное текстовое сообщение или аудио сообщение. Может быть выбрано только вместе с правом **Аудит: Исходящие сообщения**.

  В журнал аудита записывается событие "Чат" и ID пользователя WhatsApp каждого участника чата. ID локального участника предшествует ID удаленных участников.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл" и имя файла.

- **Аудит: Исходящие сообщения** - Включает аудит попыток пользователя отправить мгновенное текстовое сообщение или аудио сообщение. Может быть выбрано только вместе с правом **Аудит: Входящие сообщения**.

  В журнал аудита записывается событие "Чат" и ID пользователя WhatsApp каждого участника чата.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл" и имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных текстовых сообщений.

  Копии полученных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из WhatsApp. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных текстовых сообщений.

  Копии отправленных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в окне чата) или при выходе пользователя из WhatsApp. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

Zoom

Права аудита и теневого копирования, применимые к протоколу Zoom:

- **Аудит: Соединение** - Включает аудит попыток пользователя войти в учетную запись Zoom.

  В журнал аудита записывается событие "Соединение".

- **Аудит: Входящие сообщения** - Включает аудит попыток пользователя получить мгновенное сообщение.

  В журнал аудита записывается событие "Чат" и имена учетных записей Zoom всех участников чата. Имя локального участника предшествует именам удаленных участников.

- **Аудит: Входящие файлы** - Включает аудит попыток пользователя получить файл.

  В журнал аудита записывается событие "Входящий файл" и имя файла.

- **Аудит: Исходящие звонки** - Включает аудит попыток пользователя принять участие в какой-либо конференции Zoom.

  В журнал аудита записывается событие "Исходящий звонок" и имена учетных записей Zoom всех участников конференции. Имя локального участника предшествует именам удаленных участников.

- **Аудит: Исходящие сообщения** - Включает аудит попыток пользователя отправить мгновенное сообщение.

  В журнал аудита записывается событие "Чат" и имена учетных записей Zoom всех участников чата.

- **Аудит: Исходящие файлы** - Включает аудит попыток пользователя отправить файл.

  В журнал аудита записывается событие "Исходящий файл" и имя файла.

- **Теневое копирование: Входящие сообщения** - Включает теневое копирование полученных мгновенных сообщений.

  Копии полученных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в чате) или при выходе пользователя из приложения Zoom. Теневая копия содержит точную копию всех полученных сообщений.

- **Теневое копирование: Входящие файлы** - Включает теневое копирование полученных файлов.

  В журнал теневого копирования записываются копии полученных файлов.

- **Теневое копирование: Исходящие сообщения** - Включает теневое копирование отправленных мгновенных сообщений.

  Копии отправленных мгновенных сообщений записываются в журнал теневого копирования в виде текстовых файлов. Теневая копия сообщений записывается в журнал после отсутствия активности участников чата в течение 30 минут (т.е. спустя 30 минут с момента последнего обмена сообщениями в чате) или при выходе пользователя из приложения Zoom. Теневая копия содержит точную копию всех отправленных сообщений.

- **Теневое копирование: Исходящие файлы** - Включает теневое копирование отправленных файлов.

  В журнал теневого копирования записываются копии отправленных файлов.

Аудит и теневое копирование по умолчанию

Можно задать правила аудита и теневого копирования по умолчанию. Такие правила задаются для групп Пользователи (Users) и Все (Everyone). Следующая таблица содержит список прав, которые предоставляются этим группам по умолчанию.

Группа/ Протокол	Пользователи	Все
Поиск работы	Аудит: Соединение Аудит: Поиск Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Поиск Аудит: Исходящие сообщения Аудит: Исходящие файлы
Файловые хранилища	Аудит: Соединение Аудит: Входящие файлы Аудит: POST-запросы Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие файлы Аудит: POST-запросы Аудит: Исходящие файлы
FTP	Аудит: Соединение Аудит: Входящие файлы Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие файлы Аудит: Исходящие файлы
HTTP	Аудит: Соединение Аудит: Входящие данные Аудит: Входящие файлы Аудит: Исходящие данные Аудит: POST-запросы Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие данные Аудит: Входящие файлы Аудит: Исходящие данные Аудит: POST-запросы Аудит: Исходящие файлы
IBM Notes	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы
ICQ Messenger	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы
IRC	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы
Jabber	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы

Группа/ Протокол	Пользователи	Все
Mail.ru Агент	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы
MAPI	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы
Skype	Аудит: Соединение Аудит: Входящие звонки Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие звонки Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие звонки Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие звонки Аудит: Исходящие сообщения Аудит: Исходящие файлы
SMB	Аудит: Соединение Аудит: Входящие файлы Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие файлы Аудит: Исходящие файлы
SMTP	Аудит: Соединение Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Исходящие сообщения Аудит: Исходящие файлы
Социальные сети	Аудит: Соединение Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Исходящие сообщения Аудит: Исходящие файлы
Telegram	Аудит: Соединение Аудит: Соединение (веб) Аудит: Входящие звонки Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие звонки Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Соединение (веб) Аудит: Входящие звонки Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие звонки Аудит: Исходящие сообщения Аудит: Исходящие файлы
Telnet	Аудит: Соединение	Аудит: Соединение
Торрент	Аудит: Соединение	Аудит: Соединение
Viber	Аудит: Соединение Аудит: Входящие звонки Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие звонки Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие звонки Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие звонки Аудит: Исходящие сообщения Аудит: Исходящие файлы

Группа/ Протокол	Пользователи	Все
Web-почта	Аудит: Соединение Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Исходящие сообщения Аудит: Исходящие файлы
Web-поиск	Аудит: Поиск	Аудит: Поиск
WhatsApp	Аудит: Соединение Аудит: Соединение (веб) Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Соединение (веб) Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие сообщения Аудит: Исходящие файлы
Zoom	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие звонки Аудит: Исходящие сообщения Аудит: Исходящие файлы	Аудит: Соединение Аудит: Входящие сообщения Аудит: Входящие файлы Аудит: Исходящие звонки Аудит: Исходящие сообщения Аудит: Исходящие файлы

Действия по управлению аудитом, теневым копированием и алертами

Управление аудитом, теневым копированием и алертами для протоколов в оперативном режиме предполагает:

- Задание и редактирование правил аудита и теневого копирования
- Включение тревожных оповещений
- Сброс правил в исходное состояние

Примечание: Можно задавать правила аудита и теневого копирования для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Правила аудита и теневого копирования для оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Правила аудита и теневого копирования для автономного режима (офлайн-профиль) применяются, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Для получения дополнительной информации о политиках DeviceLock для автономного режима работы см. раздел Политики безопасности DeviceLock (офлайн-профиль). Для получения информации о том, как задать правила аудита и теневого копирования для автономного режима, см. раздел Управление правилами аудита, теневого копирования и оповещений для автономного режима.

Аудит, правила теневого копирования и алерты для оперативного режима могут иметь одно из следующих состояний:

- **Не определено** - Аудит, правила теневого копирования и тревожные оповещения для данного протокола не заданы.
- **Задано** - Для данного протокола заданы аудит, правила теневого копирования и/или тревожные оповещения.
- **Нет аудита** - Настройки для данного протокола не разрешают аудит, теневое копирование и тревожные оповещения ни для каких учетных записей.

Задание и редактирование правил аудита и теневого копирования

Чтобы задать и редактировать правила аудита и теневого копирования

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выберите **Аудит, Теневое копирование и Алерты**.

   На панели сведений отобразятся протоколы, для которых можно задавать правила аудита и теневого копирования. В столбце "Обычный" на панели сведений отображается текущее состояние правил для каждого протокола для оперативного режима.

4. На панели сведений выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши протокол, для которого требуется задать или редактировать правила, а затем выберите команду **Установить аудит, теневое копирование и алерты**.

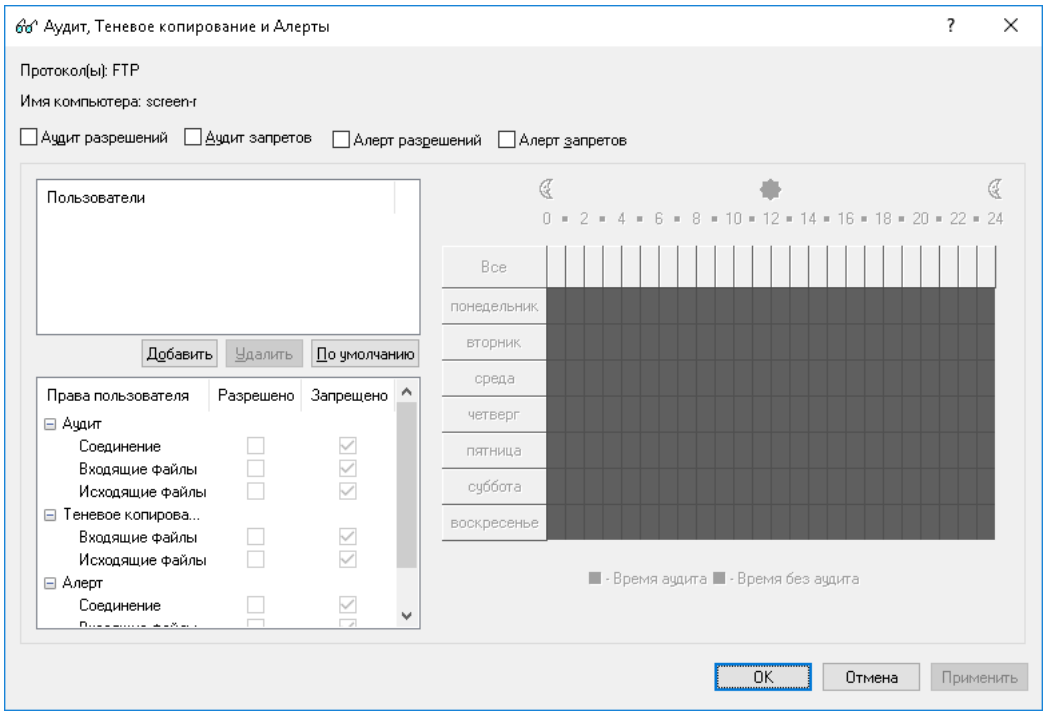
     - или -

   - Выберите протокол, для которого требуется задать или редактировать правила, а затем щелкните значок **Установить аудит, теневое копирование и алерты** на панели инструментов.

     - или -

   - Дважды щелкните протокол, для которого требуется задать или редактировать правила.

   Появится диалоговое окно "Аудит, Теневое копирование и Алерты".



5. В диалоговом окне **Аудит, Теневое копирование и Алерты** выполните следующее:

   Чтобы задать правила аудита и теневого копирования по умолчанию

   a) В левой верхней части диалогового окна укажите, какие события записываются в журнал аудита. Установите флажок **Аудит разрешений**, чтобы регистрировать успешные попытки доступа к протоколу. Установите флажок **Аудит запретов**, чтобы регистрировать неудачные попытки доступа к протоколу.

   b) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **По умолчанию**.

      По умолчанию правила аудита и теневого копирования задаются для групп Пользователи (Users) и Все (Everyone). Подробнее см. в разделе Аудит и теневое копирование по умолчанию ранее в этом документе.

Чтобы настроить правила аудита и теневого копирования для нового пользователя или группы

a) В левой верхней части диалогового окна укажите, какие события записываются в журнал аудита. Установите флажок **Аудит разрешений**, чтобы регистрировать успешные попытки доступа к протоколу. Установите флажок **Аудит запретов**, чтобы регистрировать неудачные попытки доступа к протоколу.

b) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**.

Появится диалоговое окно "Выбор: "Пользователи" или "Группы"".

c) В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.

Добавленные пользователи и группы отображаются в области "Пользователи" в левой верхней части диалогового окна "Аудит, Теневое копирование и Алерты".

d) В левой верхней части диалогового окна **Аудит, Теневое копирование и Алерты** в области **Пользователи** выберите пользователя или группу.

Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

e) На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права (см. Права аудита и теневого копирования).

В правой части диалогового окна "Аудит, Теневое копирование и Алерты" можно указать дни недели и время (например, с 7 часов утра до 5 часов вечера с понедельника по пятницу), когда действия выбранных пользователей будут записываться в журнал аудита или теневого копирования. Используйте левую кнопку мыши, чтобы выбрать дни недели и время, когда действия выбранных пользователей будут записываться в журнал. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда действия пользователей не будут записываться в журнал.

Чтобы изменить правила аудита и теневого копирования для имеющегося пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу.

b) На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

Чтобы удалить имеющегося пользователя или группу и правило

- В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или клавишу DELETE.

  При удалении пользователя или группы удаляются также и правила, связанные с этим пользователем или группой.

6. Нажмите кнопку **OK** или **Применить**.

Включение тревожных оповещений

Вы можете включить тревожные оповещения, которые будут рассылаться при попытке пользователя обратиться к протоколу определенного типа.

DeviceLock рассылает тревожные оповещения с учетом соответствующих настроек. В этих настройках задается адресат и способ отправки оповещений. Перед тем, как включить оповещения для определенных событий, задайте параметры оповещений в настройках сервиса DeviceLock (см. раздел Алерты).

Оповещения о событиях, связанных с доступом, можно включить в диалоговом окне **Аудит, Теневое копирование и Алерты**. Оповещения включаются так же, как задаются правила аудита (см. раздел Задание и редактирование правил аудита и теневого копирования), в следующем порядке:

- Укажите, для каких событий необходимо рассылать оповещения. Оповещения можно настроить для попыток доступа к устройству (как удачных, так и неудачных). Установите флажок **Алерт разрешений**, чтобы включить оповещения об успешных попытках доступа к устройству. Установите флажок **Алерт запретов**, чтобы включить оповещения о неудачных попытках доступа к протоколу.
- Укажите пользователей и/или группы, на действия которых будут рассылаться оповещения. Для этого в левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.
- Укажите, на какие действия пользователей нужно рассылать оповещения, а на какие нет. В левой верхней части диалогового окна в области **Пользователи** выберите добавленного пользователя или группу. На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить право на оповещение. Права на оповещения определяют, на какие действия пользователя с протоколами следует рассылать оповещения. Права на оповещение аналогичны правам на аудит. Единственное различие состоит в том, что когда происходят события, удовлетворяющие определенным критериям, DeviceLock отправляет оповещение, а не протоколирует их в журнале аудита. Подробнее о правах аудита для протоколов см. в разделе Права аудита и теневого копирования.
- Укажите дни и часы (например, с 7 утра до 5 вечера с понедельника по пятницу), в которые оповещения о действиях пользователя с протоколами будут или не будут рассылаться. Для этого на правой панели диалогового окна выберите дни и часы левой кнопкой мыши. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда на действия пользователей не будут рассылаться оповещения.

Примечание: Можно настроить различные параметры оповещений для оперативного и автономного режимов. Оперативные оповещения (обычный профиль) создаются, когда клиентские компьютеры подключены к сети. Автономные оповещения (офлайн-профиль) создаются, когда клиентские компьютеры работают в автономном режиме. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Для получения дополнительной информации о политиках DeviceLock для автономного режима работы, см. раздел Политики безопасности DeviceLock (офлайн-профиль). Для получения информации о включении оповещений для автономного режима см. раздел Управление правилами аудита, теневого копирования и оповещений для автономного режима.

Сброс правил в исходное состояние

Если для развертывания политик DeviceLock используется DeviceLock Group Policy Manager или DeviceLock Service Settings Editor, могут возникнуть ситуации, когда требуется отменить применение заданных правил аудита и теневого копирования к определенной группе компьютеров. Для этого необходимо вернуть ранее заданные правила в исходное "неопределенное" состояние. Все параметры DeviceLock, которые установлены в состояние "не определен", игнорируются на клиентских компьютерах.

Чтобы сбросить правила в исходное "неопределенное" состояние

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.
   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выберите **Аудит, Теневое копирование и Алерты**.

   Если в дереве консоли выбрать "Аудит, Теневое копирование и Алерты", на панели сведений отобразятся протоколы, для которых можно задавать правила аудита и теневого копирования.
4. На панели сведений щелкните правой кнопкой мыши протокол, для которого требуется вернуть правила в исходное "неопределенное" состояние, а затем выберите команду **Сбросить**.

   Можно вернуть правила в исходное "неопределенное" состояние для нескольких протоколов одновременно. Чтобы это сделать, выполните следующее:
   a) На панели сведений выберите несколько протоколов, удерживая клавишу SHIFT или CTRL и щелкая протоколы.
   b) Щелкните правой кнопкой мыши выбранные протоколы, и выберите команду **Сбросить**.

Белый список протоколов

Белый список сетевых протоколов позволяет выборочно разрешать передачу данных по сети через поддерживаемые протоколы, несмотря на установленные настройки блокирования доступа к протоколам. Белый список наиболее эффективен для реализации сценария "минимальные привилегии", когда администратор блокирует трафик по всем протоколам, а затем предоставляет пользователям доступ только к тем ресурсам, которые необходимы для работы. В белом списке можно идентифицировать ресурсы по адресам IPv4 или IPv6.

Например, можно запретить всем пользователям доступ к протоколам SMTP и Web-почта, а затем использовать белый список, чтобы разрешить определенным пользователям отправлять электронную почту на указанные адреса электронной почты. Применение таких политик безопасности снижает риск утечки и кражи данных.

Под узлом **Протоколы** > **Белый список** в дереве консоли перечисляются пользователи и группы, для которых задан белый список протоколов. Протоколы в белом списке могут быть заданы индивидуально для каждого пользователя и группы.

Контекстное меню белого списка протоколов содержит следующие команды:

- **Удалить пользователя** - Удаляет пользователя или группу из белого списка.
- **Управление** - Открывает диалоговое окно, позволяющее задать или отредактировать белый список для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее задать или отредактировать белый список для автономного режима.
- **Загрузить** - Позволяет импортировать ранее сохраненный файл с белым списком протоколов для оперативного режима.
- **Загрузить офлайновые настройки** - Позволяет импортировать ранее сохраненный файл с белым списком протоколов для автономного режима.
- **Сохранить** - Позволяет экспортировать белый список протоколов, заданный для оперативного режима, в файл с расширением `.pwl`, который затем можно импортировать и использовать на другом компьютере.
- **Сохранить офлайновые настройки** - Позволяет экспортировать белый список протоколов, заданный для автономного режима, в файл с расширением `.pwl`, который затем можно импортировать и использовать на другом компьютере.
- **Сбросить** - Сбрасывает белый список протоколов для оперативного режима в состояние "не задано". Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.
- **Сбросить офлайновые настройки** - Сбрасывает список протоколов для автономного режима в состояние "не задано". Если такой белый список не задан, к клиентским компьютерам, находящимся не в сети, применяется белый список, заданный для оперативного режима.
- **Удалить офлайновые настройки** - Блокирует наследование белого списка, заданного для автономного режима, и принудительно применяет белый список, заданный для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

Дополнительные сведения см. в разделе Действия по управлению белым списком.

Правила белого списка

Если выбрать пользователя или группу под узлом **Протоколы** > **Белый список** в дереве консоли, на панели сведений отображаются правила белого списка, заданные для этого пользователя или группы. Для каждого правила список содержит следующие сведения:

- **Протокол** - Протокол, к которому применяется правило.
- **Имя** - Имя правила.
- **Хосты** - Разрешенные узлы.
- **Порты** - Разрешенные порты.
- **Отправить алерт** - Настройка отправки алертов данным правилом. Отправка может быть включена или отключена, либо эта настройка может наследоваться от протокола.
- **Протоколировать событие** - Настройка протоколирования событий аудита данным правилом. Протоколирование может быть включено или отключено, либо эта настройка наследуется от протокола.
- **Теневое копирование** - Настройка теневого копирования данным правилом. Теневое копирование может быть включено или отключено, либо эта настройка наследуется от протокола.
- **SSL** - Настроенный параметр SSL. Возможные значения:
  - **Разрешено** - Разрешает SSL-соединения.
  - **Запрещено** - Запрещает SSL-соединения.
  - **Обязательно** - Требует использования SSL для всех соединений.
- **Контентный анализ** - Отображает, включена ли проверка контента.
- **Дополнительные параметры** - Следующие параметры, связанные с протоколом:
  - **От** - Разрешенные идентификаторы отправителей мгновенных сообщений и адреса электронной почты, с которых разрешена отправка сообщений.
  - **Кому** - Разрешенные идентификаторы получателей мгновенных сообщений и адреса электронной почты, для которых разрешено получение сообщений.
- **Профиль** - Возможные значения:
  - **Обычный** - Правило применяется к клиентским компьютерам, находящимся в сети.
  - **Офлайн** - Правило применяется к клиентским компьютерам, работающим автономно.

  Можно задавать белый список протоколов для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Для получения информации о том, как задать белый список протоколов для автономного режима, см. раздел Управление белым списком протоколов для автономного режима.

Контекстное меню правила в списке на панели сведений содержит следующие команды:

- **Управление** - В зависимости от профиля данного правила (обычный или офлайн), открывает диалоговое окно, в котором можно задать белый список протоколов для оперативного или автономного режима.
- **Редактировать** - Открывает диалоговое окно, в котором можно просмотреть или изменить правило белого списка.
- **Отправить алерт** - Включает или отключает отправку алертов для данного правила.
- **Протоколировать событие** - Включает или отключает протоколирование событий для данного правила.
- **Удалить** - Удаляет данное правило.

Подробнее см. в разделе Действия по управлению белым списком.

Параметры правил белого списка

Белый список состоит из правил, заданных для определенных сетевых протоколов. В каждом правиле указываются пользователи и группы, к которым применяется это правило, и задается набор параметров. Эти параметры делятся на две категории: общие параметры, которые применимы ко всем протоколам, и параметры, зависящие от выбора протокола.

Общие параметры:

- **Имя** - Задает имя правила.
- **Протокол** - Задает протокол, к которому применяется правило. Поддерживаются следующие протоколы: Любой, Поиск работы, Файловые хранилища, FTP, HTTP, IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMB, SMTP, Социальные сети, SSL, Telnet, Viber, Web-почта, Web-поиск и Zoom. Правила белого списка для протокола Любой дают возможность разрешить клиентам подключаться к определенным узлам и/или портам независимо от используемого сетевого протокола.

  Примечание:
  - Подключения, разрешенные правилом белого списка для протокола Любой, не блокируются правилами IP-файрвола.
  - Если протокол Viber не разрешен настройками разрешений для протоколов, правила белого списка для него не действуют. В этом случае пользователи Viber не могут отправлять и получать сообщения и файлы.
  - Если протокол HTTP не разрешен настройками разрешений для протоколов, возможны сбои при подключении к почтовой службе Zimbra или Outlook Web App (OWA), несмотря на разрешение протокола Web-почта. Для предотвращения сбоев в такой ситуации внесите хосты Zimbra и OWA в белый список для протокола HTTP.

Параметры, зависящие от выбора протокола:

- Контентный анализ
- Если правило срабатывает
- Хосты
- Порты
- Файловые хранилища
- SSL
- ID-локального отправителя
- ID-удаленного получателя
- E-mail локального отправителя
- E-mail удаленного получателя
- Социальные сети
- Сервисы Web-почты
- Сервисы Web-поиска
- Сервисы поиска работы

Контентный анализ

Параметр **Контентный анализ** применяется ко всем протоколам, кроме протоколов Любой, SSL и Telnet.

Этот параметр определяет, следует ли включить проверку контента для соединений из белого списка в соответствии с контентно-зависимыми правилами (см. раздел Правила для протоколов главы Контентно-зависимые правила (обычный профиль)). Если флажок **Контентный анализ** не установлен или контентно-зависимое правило не задано для данного подключения, то проверка контента не выполняется.

Если правило срабатывает

Параметр **Если правило срабатывает** применяется ко всем протоколам.

Этот параметр задает следующие дополнительные операции, которые будут выполняться при срабатывании правила:

- **Отправить алерт** - Оповещение рассылается при каждом срабатывании правила.

  DeviceLock рассылает оповещения с учетом настроек оповещений. В этих настройках задается адресат и способ отправки оповещений. Перед включением оповещений для правила белого списка задайте параметры оповещений в настройках сервиса DeviceLock (см. раздел Алерты).

- **Протоколировать событие** - Событие регистрируется в журнале аудита при каждом срабатывании правила.
- **Теневое копирование** - Теневая копия данных создается при каждом срабатывании правила.

При включении или отключении алертов, аудита и/или теневого копирования в правиле белого списка настройка правила имеет приоритет над соответствующей настройкой для протокола.

Пример: Если аудит включен для некоторого протокола и отключен в правиле для этого протокола, срабатывание такого правила не вызовет события аудита. Если же аудит в правиле включен, то срабатывание правила вызовет событие аудита, даже если аудит отключен на уровне протокола.

Правило может наследовать настройку алертов, аудита и/или теневого копирования, заданную для протокола. Эта опция выбрана по умолчанию и представлена неопределенным состоянием соответствующих флажков (не установленных и не очищенных). Состояние каждого флажка можно изменить независимо от других.

Пример: Если правило наследует настройку аудита, заданную для протокола, то срабатывание такого правила вызовет событие аудита только если аудит включен для протокола, контролируемого этим правилом.

Просмотрщик журнала аудита отображает следующую информацию о событиях, вызваных срабатыванием правила белого списка:

- **Тип** - `Успех`
- **Дата/Время** - Дата и время создания соединения в следующем формате: дд.мм.гггг чч:мм:сс. Пример: `05.06.2012 14:54:46`
- **Источник** - Тип протокола.
- **Действие** - Тип пользовательского действия: `Входящее соединение` либо `Исходящее соединение`
- **Имя** - Пустое поле.
- **Информация** - IP-адрес, номер порта и полное доменное имя (FQDN) удаленного узла. Пример: `Удаленный хост: 192.168.100.10:99 (computer.group.domain.com)`
- **Причина** - Причина возникновения события: `Белый список: "<имя_правила>"`
- **Пользователь** - Имя пользователя, связанного с данным событием, в следующем формате: <имя_домена>\<имя_пользователя>.
- **PID** - Идентификатор процесса приложения, связанного с событием. Пример: `4420`
- **Процесс** - Полный путь к исполняемому файлу процесса. Пример: `C:\Program Files\AppFolder\AppName.exe`

Хосты

Параметр **Хосты** применяется к следующим протоколам: Любой, FTP, HTTP, IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, SMB, SMTP, SSL и Telnet.

Этот параметр задает список узлов, разрешенных для этого правила. Если этот список задан, указанные узлы не будут блокироваться.

Узлы можно указать в любом из следующих форматов:

- DNS-имя (например, `company.com`). В DNS-имени можно использовать звездочку (*). Например, имя `*.company.com` означает любой сервер, имя которого заканчивается на `.company.com`. Для протокола HTTP в поле **Хосты** можно указывать не только адреса веб-сайтов, но и адреса отдельных веб-страниц. Таким образом можно, например, добавить в белый список только страницы по адресу `company.com/section/page`.
- Например, в качестве хоста можно указать адрес `company.com/section/page`, чтобы разрешить доступ только к страницам по этому адресу.

  Внимание: Поскольку DeviceLock использует для разрешения имен локальный файл `Hosts`, злоумышленник с правами локального администратора может изменить этот файл, чтобы обойти политику безопасности DeviceLock. Например, если белый список разрешает HTTP-доступ к сайту `company.com`, такой злоумышленник может получить доступ к запрещенному сайту `www.ru`, добавив запись `194.87.0.50 company.com` в локальный файл `Hosts`. В целях безопасности рекомендуется защитить файл `Hosts`, установив флажок **Предотвращать изменения в системных файлах настроек** в настройках параметра Администраторы DeviceLock в узле консоли Настройки сервиса.

- IPv4-адрес (например, `12.13.14.15`). Можно указать диапазон IPv4-адресов, разделенных дефисом (-) (например, `12.13.14.18-12.13.14.28`). Также можно указывать маски подсети в следующем формате: `<IPv4-адрес>/<длина маски подсети в битах>` (например, `3.4.5.6/16`).
- IPv6-адрес, например `fe80:0000:0000:0000:0a2f:7e00:0004:533a`, `fe80:0:0:0:a2f:7e00:4:533a` или `fe80::a2f:7e00:4:533a`.

Чтобы задать несколько узлов, можно разделять их запятой (,) или точкой с запятой (;) или нажимать клавишу ENTER после ввода каждой строчки. Узлы можно указывать в различных форматах, описанных выше (например, `www.microsoft.com; 12.13.14.15, 12.13.14.18-12.13.14.28`).

При добавлении узлов в белый список необходимо учитывать следующее:

- Если объекты на веб-странице (изображения, скрипты, видео, Flash-файлы, ActiveX и т.д.) загружаются с других узлов, необходимо добавить эти узлы в белый список для корректного отображения страницы.
- Если в белом списке указаны узлы, но не указаны порты, эти узлы будут доступны по всем возможным портам.
- Приложения со встроенными SSL-сертификатами (например, Dropbox, Яндекс.Диск, Google Drive, iTunes Google contacts synchronization module и др.) не смогут соединиться со своим сервером, если модуль NetworkLock активен. Модуль NetworkLock становится активным, если заданы настройки для сетевых протоколов. Чтобы исключить эту проблему, необходимо добавить сервер в белый список для протокола SSL. Чтобы узнать имена/адреса сервера, можно использовать приложение TcpView. Добавление сервера в белый список отключает контроль доступа, аудит, теневое копирование и контентную фильтрацию для всего SSL-трафика между приложением и указанным сервером.
- При запуске Outlook соединяется с сервером Exchange и контроллером домена. Если задать разрешение "Нет доступа" для протокола MAPI, а затем добавить правило белого списка для MAPI, необходимо указать имя узла сервера Exchange и имя узла контроллера домена во избежание затруднений.

  Это также относится к клиенту IBM Notes, серверу IBM Domino и именам соответствующих контроллеров домена.

Порты

Параметр **Порты** применяется к следующим протоколам: Любой, FTP, HTTP, ICQ Messenger, IRC, Jabber, Mail.ru Агент, SMTP, SSL и Telnet.

Этот параметр задает порт или порты, открытые для этого правила. Если этот список задан, указанные порты не будут блокироваться.

Можно указать отдельный порт или диапазон портов, разделенных дефисом (-). Например, чтобы открыть порт 25, укажите `25`. Чтобы открыть порты с 5000 по 5020 включительно, укажите `5000-5020`. Чтобы указать несколько портов, можно разделять их запятой (,) или точкой с запятой (;). Например `25, 36; 8080, 5000-5020`. Также можно нажимать клавишу ENTER после ввода каждой строчки.

Примечание: Если в белом списке указаны порты, но не указаны узлы, пользователи получат доступ ко всем узлам, доступным через указанные порты.

Файловые хранилища

Этот параметр применяется к протоколу Файловые хранилища.

Параметр **Файловые хранилища** задает список разрешенных служб файлового обмена и синхронизации для данного правила. Если список задан, передача информации через службы, указанные в этом списке, не блокируется. Перечень поддерживаемых служб см. в описании протокола Файловые хранилища.

SSL

Параметр **SSL** применяется к следующим протоколам: Файловые хранилища, FTP, HTTP, ICQ Messenger, IRC, SMTP и Web-почта.

Этот параметр устанавливает требования к SSL-соединениям. Доступны следующие варианты:

- **Разрешено** - Разрешает SSL-соединения.
- **Запрещено** - Запрещает SSL-соединения.
- **Обязательно** - Требует использования SSL для всех соединений.

ID-локального отправителя

Параметр **ID-локального отправителя** применяется к следующим протоколам: ICQ Messenger, Jabber, Mail.ru Агент, Skype, Viber и Zoom.

Данный параметр задает список идентификаторов пользователей, имеющих право отправлять сообщения и файлы, а также совершать звонки. Если этот список задан, DeviceLock не будет блокировать сообщения, файлы и звонки, исходящие от указанных пользователей.

Если идентификаторов несколько, их следует разделять запятой (,) или точкой с запятой (;). Также можно нажимать клавишу ENTER после ввода каждого идентификатора или группы идентификаторов.

Можно использовать звездочку (*) в качестве подстановочного знака для обозначения любого набора символов или знак вопроса (?) для обозначения любого одиночного символа. Также можно указать в этом поле одну только звездочку, что будет означать "любых отправителей".

Пользователи ICQ Messenger идентифицируются по номерам UIN (например, `111222`). Пользователи Jabber идентифицируются по идентификаторам Jabber в формате `<user>@<domain>`. Пользователи Mail.ru Агент идентифицируются по адресам электронной почты в формате `<user>@mail.ru`. Пользователи Skype идентифицируются по именам учетных записей Skype. Пользователи Viber идентифицируются по ID пользователя Viber (например, `12345550809`). Пользователи Zoom идентифицируются по ID пользователя Zoom (например, `1236567390` или `john@host.net`).

ID-удаленного получателя

Параметр **ID-удаленного получателя** применяется к следующим протоколам: ICQ Messenger, Jabber, Mail.ru Агент, Skype, Viber и Zoom.

Данный параметр задает список идентификаторов пользователей, имеющих право получать сообщения и файлы, а также принимать звонки. Если этот список задан, DeviceLock не будет блокировать сообщения, файлы и звонки, направленные указанным пользователям.

Если идентификаторов несколько, их следует разделять запятой (,) или точкой с запятой (;). Также можно нажимать клавишу ENTER после ввода каждого идентификатора или группы идентификаторов.

Можно использовать звездочку (*) в качестве подстановочного знака для обозначения любого набора символов или знак вопроса (?) для обозначения любого одиночного символа. Также можно указать в этом поле одну только звездочку, что будет означать "любых получателей".

Пользователи ICQ Messenger идентифицируются по номерам UIN (например, `111222`). Пользователи Jabber идентифицируются по идентификаторам Jabber в формате `<user>@<domain>`. Пользователи Mail.ru Агент идентифицируются по адресам электронной почты в формате `<user>@mail.ru`. Пользователи Skype идентифицируются по именам учетных записей Skype. Пользователи Viber идентифицируются по ID пользователя Viber (например, `12345550809`). Пользователи Zoom идентифицируются по ID пользователя Zoom (например, `1236567390` или `john@host.net`).

E-mail локального отправителя

Параметр **E-mail локального отправителя** применяется к следующим протоколам: IBM Notes, MAPI, SMTP и Web-почта.

Этот параметр задает список адресов электронной почты, с которых разрешена отправка сообщений. Если этот список задан, отправка сообщений с указанных адресов не будет блокироваться. Адреса электронной почты указываются в формате `<user>@<domain>` (или `<user>/<domain>` для IBM Notes).

Если адресов несколько, их следует разделять запятой (,) или точкой с запятой (;). Также можно нажимать клавишу ENTER после ввода каждого адреса или группы адресов.

Можно использовать звездочку (*) в качестве подстановочного знака для обозначения любого набора символов или знак вопроса (?) для обозначения любого одиночного символа. Также в адресе электронной почты можно указать одну только звездочку перед или после символа “собака” (@). Например, чтобы разрешить отправку писем от всех пользователей в данном домене, введите `*@domain` (или `*/domain` для IBM Notes).

Примечание: При добавлении адресов электронной почты получателей и отправителей в белый список для протокола Web-почта, необходимо учесть следующее: письма, отправленные через веб-интерфейс, хранятся в серверной папке **Отправленные** и могут пересылаться на любой адрес с любого компьютера.

E-mail удаленного получателя

Параметр **E-mail удаленного получателя** применяется к следующим протоколам: IBM Notes, MAPI, SMTP и Web-почта.

Этот параметр задает список адресов электронной почты, на которые возможна отправка сообщений. Если этот список задан, отправка сообщений для указанных адресов не будет блокироваться. Адреса электронной почты указываются в формате `<user>@<domain>` (или `<user>/<domain>` для IBM Notes).

Если адресов несколько, их следует разделять запятой (,) или точкой с запятой (;). Также можно нажимать клавишу ENTER после ввода каждого адреса или группы адресов.

Можно использовать звездочку (*) в качестве подстановочного знака для обозначения любого набора символов или знак вопроса (?) для обозначения любого одиночного символа. Также в адресе электронной почты можно указать одну только звездочку перед или после символа «собака» (@). Например, чтобы разрешить отправку писем всем пользователям в данном домене, введите `*@domain` (или `*/domain` для IBM Notes).

Социальные сети

Параметр **Социальные сети** применяется к протоколу Социальные сети.

Этот параметр задает список разрешенных сайтов социальных сетей для данного правила. Если этот список задан, указанные сайты не будут блокироваться. Перечень поддерживаемых сайтов социальных сетей см. в описании протокола Социальные сети.

Сервисы Web-почты

Параметр **Сервисы Web-почты** применяется к протоколу Web-почта.

Этот параметр задает список разрешенных служб веб-почты. Если список задан, сообщения электронной почты, отправляемые через указанные почтовые веб-службы, не будут блокироваться. Перечень поддерживаемых почтовых веб-служб см. в описании протокола Web-почта.

Сервисы Web-поиска

Параметр **Сервисы Web-поиска** применяется к протоколу Web-поиск.

Этот параметр задает список разрешенных провайдеров веб-поиска. Если список задан, то сервис DeviceLock не будет блокировать поисковые запросы к провайдерам, выбранным в этом списке. Перечень поддерживаемых провайдеров см. в описании протокола Web-поиск.

Сервисы поиска работы

Параметр **Сервисы поиска работы** применяется к протоколу Поиск работы.

Этот параметр задает список разрешенных провайдеров веб-поиска работы. Если список задан, то сервис DeviceLock не будет блокировать запросы к провайдерам, выбранным в этом списке. Перечень поддерживаемых провайдеров см. в описании протокола Поиск работы.

Действия по управлению белым списком

Управление белым списком протоколов для оперативного режима предполагает:

- Задание белого списка протоколов
- Редактирование правил белого списка протоколов
- Копирование правил белого списка протоколов
- Экспорт и импорт белого списка протоколов
- Сброс белого списка протоколов в исходное состояние
- Удаление правил белого списка протоколов

Примечание: Можно задавать различные белые списки протоколов для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Белый список протоколов для оперативного режима (обычный профиль) применяется, когда клиентские компьютеры находятся в сети. Белый список протоколов для автономного режима (офлайн-профиль) применяется, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Подробнее о политиках DeviceLock для автономного режима работы см. в разделе Политики безопасности DeviceLock (офлайн-профиль). Для получения информации о том, как задать белый список протоколов для автономного режима, см. раздел Управление белым списком протоколов для автономного режима.

Задание белого списка протоколов

Чтобы задать белый список протокола

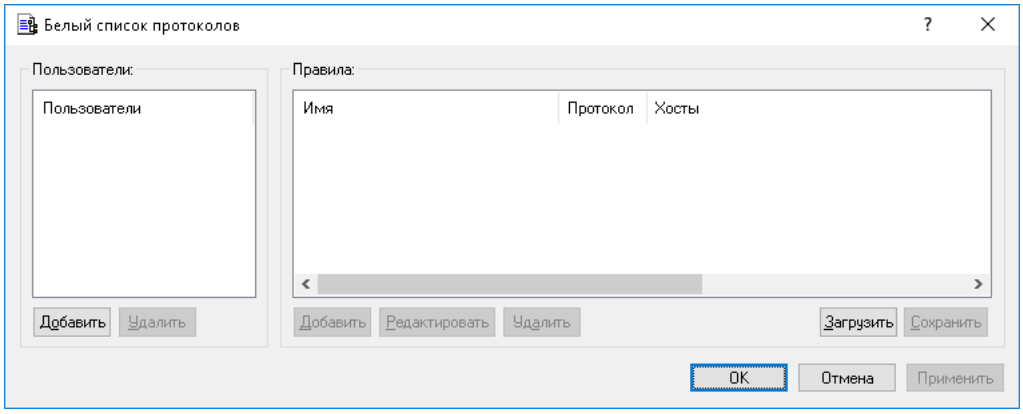
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление**.

     - или -
   - Выберите **Белый список**, а затем щелкните значок **Управление** на панели инструментов.

Появится диалоговое окно “Белый список протоколов”.



4. В левой части диалогового окна **Белый список протоколов** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

5. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать белый список протоколов, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой части диалогового окна “Белый список протоколов”.

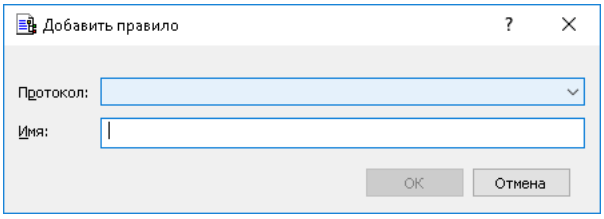
   Чтобы удалить пользователя или группу, в левой части диалогового окна **Белый список протоколов** в области **Пользователи**, выберите пользователя или группу, а затем нажмите кнопку **Удалить**.

6. В левой части диалогового окна **Белый список протоколов** в области **Пользователи** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

7. В правой части диалогового окна **Белый список протоколов** в области **Правила** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Добавить правило”.



8. В диалоговом окне **Добавить правило** задайте параметры правила.

   Вначале задайте общие параметры:

   - Чтобы задать протокол, выберите его в списке **Протокол**.
   - Чтобы задать имя правила, ведите его в поле **Имя**.

Затем задайте параметры, зависящие от выбранного протокола:

- Чтобы включить проверку контента, установите флажок **Контентный анализ**. Подробнее см. в описании параметра Контентный анализ.
- Чтобы указать дополнительные действия, которые будут выполняться при срабатывании правила, установите соответствующие флажки в области **Если правило срабатывает**. Подробнее см. в описании параметра Если правило срабатывает.
- Чтобы указать узлы, в поле **Хосты** введите имена узлов или IP-адреса через запятую или точку с запятой. Подробнее см. в описании параметра Хосты.
- Чтобы указать порты, в поле **Порты** введите номера портов через запятую или точку с запятой. Подробнее см. в описании параметра Порты.
- Чтобы указать службы файлового обмена и синхронизации, в области **Файловые хранилища** установите соответствующие флажки. Подробнее см. в описании параметра Файловые хранилища.
- Чтобы настроить параметры SSL, в области **SSL** выберите один из следующих вариантов: **Разрешено** (разрешает SSL-соединения), **Запрещено** (запрещает SSL-соединения) или **Обязательно** (требует использования SSL для всех соединений).
- Чтобы указать идентификаторы локальных отправителей мгновенных сообщений, в поле **ID-локального отправителя** введите идентификаторы пользователей через запятую или точку с запятой. Подробнее см. в описании параметра ID-локального отправителя.
- Чтобы указать получателей мгновенных сообщений, в поле **ID-удаленного получателя** введите идентификаторы пользователей через запятую или точку с запятой. Подробнее см. в описании параметра ID-удаленного получателя.
- Чтобы указать отправителей электронной почты, в поле **E-mail локального отправителя** введите адреса электронной почты через запятую или точку с запятой. Подробнее см. в описании параметра E-mail локального отправителя.
- Чтобы указать получателей электронной почты, в поле **E-mail удаленного получателя** введите адреса электронной почты через запятую или точку с запятой. Подробнее см. в описании параметра E-mail удаленного получателя.
- Чтобы указать сайты социальных сетей, установите соответствующие флажки в области **Социальные сети**. Подробнее см. в описании параметра Социальные сети.
- Чтобы указать службы веб-почты, установите соответствующие флажки в области **Сервисы Web-почты**. Подробнее см. в описании параметра Сервисы Web-почты.
- Чтобы указать провайдеров веб-поиска, установите соответствующие флажки в области **Сервисы Web-поиска**. Подробнее см. в описании параметра Сервисы Web-поиска.
- Чтобы указать провайдеров веб-поиска работы, установите соответствующие флажки в области **Сервисы поиска работы**. Подробнее см. в описании параметра Сервисы поиска работы.

9. Нажмите кнопку **OK**.

   Созданное правило появится в области "Правила" в правой части диалогового окна "Белый список протоколов".

10. Нажмите кнопку **OK** или **Применить**.

    Пользователи и группы, для которых применяются правила белого списка, отображаются в узле "Белый список" дерева консоли.

Если в дереве консоли выбрать пользователя или группу, к которой применяется правило белого списка, на панели сведений отобразится информация о заданном правиле (подробнее см. в разделе Правила белого списка).

Редактирование правил белого списка протоколов

Можно изменять значения параметров, настроенных для правила белого списка, в любое время.

Чтобы редактировать правило белого списка протоколов

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** щелкните правой кнопкой мыши **Белый список**, выберите команду **Управление**, а затем выполните следующие действия:

   a) В левой части диалогового окна **Белый список протоколов** в области **Пользователи**, выберите пользователя или группу, для которого требуется изменить правило.

   Если выбрать пользователей или группы, в области "Правила" в правой части диалогового окна отобразятся правила белого списка, которые применяются к этим пользователям или группам.

   b) В правой части диалогового окна **Белый список протоколов** в области **Правила** выберите правило, которое требуется редактировать, а затем нажмите кнопку **Редактировать**.

   - или -

   Щелкните правой кнопкой мыши правило, а затем выберите команду **Редактировать**.

   - или -

   В узле **Протоколы**, раскройте узел **Белый список**, а затем выполните следующие действия:

   a) В узле **Белый список** выберите пользователя или группу, для которого требуется изменить правило.

   Если выбрать пользователей или группы, на панели сведений отобразятся правила белого списка, которые применяются к этим пользователям или группам.

   b) На панели сведений щелкните правой кнопкой мыши правило, которое требуется редактировать, а затем выберите команду **Редактировать**.

   - или -

   На панели сведений дважды щелкните правило, которое требуется редактировать.

   Появится диалоговое окно "Редактирование правила".

4. В диалоговом окне **Редактирование правила** внесите необходимые изменения.

5. Нажмите кнопку **OK**, чтобы применить изменения.

Копирование правил белого списка протоколов

Можно выполнять операции вырезать-вставить, копировать-вставить, а также операции перетаскивания, чтобы повторно использовать существующие правила белого списка протоколов.

Чтобы скопировать правило белого списка

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление**.

     - или -

   - Выберите **Белый список**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно “Белый список протоколов”.

4. В левой части диалогового окна **Белый список протоколов** в области **Пользователи** выберите пользователя или группу, к которой применяется правило, которое требуется скопировать.

   Если выбрать пользователей или группы, в области “Правила” в правой части диалогового окна отобразятся правила белого списка, которые применяются к этим пользователям или группам.

5. В правой части диалогового окна **Белый список протоколов** в области **Правила** щелкните правой кнопкой мыши правило, которое требуется скопировать, а затем выберите команду **Копировать** или **Вырезать**.

   Вырезанное или скопированное правило автоматически копируется в буфер обмена.

   Также можно использовать сочетания клавиш CTRL+C, CTRL+X и CTRL+V, чтобы скопировать, вырезать и вставить правило. При нажатии CTRL+X правило будет вырезано только после того, как вы его вставите.

6. В левой части диалогового окна **Белый список протоколов** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно Выбор: “"Пользователи" или "Группы"”.

7. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых должно применяться скопированное правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой части диалогового окна “Белый список протоколов”.

8. В левой части диалогового окна **Белый список протоколов** в области **Пользователи** выберите пользователей или группы, для которых требуется задать скопированное правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

9. В правой части диалогового окна **Белый список протоколов** щелкните правой кнопкой мыши в области **Правила**, а затем выберите команду **Вставить**.

   Скопированное правило отображается в области "Правила" в правой части диалогового окна "Белый список протоколов".

10. Нажмите кнопку **OK** или **Применить**, чтобы применить скопированное правило.

Экспорт и импорт белого списка протоколов

Можно экспортировать все заданные правила белого списка протоколов в файл с расширением `.pwl`, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт правил также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать белый список протоколов

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Сохранить**.

     - или -

   - Выберите **Белый список**, а затем щелкните значок **Сохранить** на панели инструментов.

     - или -

   - Раскройте **Белый список**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Сохранить**.

     - или -

   - Раскройте **Белый список**, выберите любого пользователя или группу, указанную в белом списке. На панели сведений щелкните правой кнопкой правило белого списка, а затем выберите команду **Сохранить**.

     - или -

- Раскройте **Белый список**, выберите любого пользователя или группу, указанную в белом списке, а затем щелкните значок **Сохранить** на панели инструментов.

  - или -

- Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление.** В правой части диалогового окна **Белый список протоколов** в области **Правила** нажмите кнопку **Сохранить**.

4. В появившемся диалоговом окне выберите папку, в которую требуется сохранить файл, задайте имя файла, и нажмите кнопку **Сохранить**.

   При экспорте белый список протоколов сохраняется в файле с расширением .pwl.

Чтобы импортировать белый список протоколов

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Загрузить**.

     - или -

   - Выберите **Белый список**, а затем щелкните значок **Загрузить** на панели инструментов.

     - или -

   - Раскройте **Белый список**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Загрузить**.

     - или -

   - Раскройте **Белый список**, выберите любого пользователя или группу, указанную в белом списке. На панели сведений щелкните правой кнопкой мыши любое правило белого списка, а затем выберите команду **Загрузить**.

     - или -

   - Раскройте **Белый список**, выберите любого пользователя или группу, указанную в белом списке, а затем щелкните значок **Загрузить** на панели инструментов.

     - или -

   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление.** В правой части диалогового окна **Белый список протоколов** в области **Правила** нажмите кнопку **Загрузить**.

4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

   Если белый список протоколов уже настроен и вы импортируете новый белый список, появится следующее сообщение: "Вы хотите перезаписать существующие записи (Да - перезаписать, Нет - добавить)?" В окне сообщения нажмите кнопку "Да", чтобы перезаписать существующий белый список. Нажмите кнопку "Нет", чтобы добавить новый список к старому.

Сброс белого списка протоколов в исходное состояние

Если для развертывания политик DeviceLock используется DeviceLock Group Policy Manager или DeviceLock Service Settings Editor, могут возникнуть ситуации, когда потребуется отменить применение заданного белого списка протоколов к определенной группе компьютеров. Для этого необходимо вернуть ранее заданный белый список в исходное "неопределенное" состояние. Все параметры DeviceLock, которые установлены в состояние "не определен", игнорируются на клиентских компьютерах.

Чтобы сбросить белый список протоколов в исходное "неопределенное" состояние

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.
   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Сбросить**.

Удаление правил белого списка протоколов

Можно удалять отдельные правила белого списка протоколов, если они больше не нужны.

Чтобы удалить правило белого списка

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Раскройте **Белый список**, щелкните правой кнопкой мыши пользователя или группу, для которой задано правило, а затем выберите команду **Удалить пользователя**.

     Если удалить пользователя или группу, все правила, заданные для этого пользователя или группы, автоматически удалятся.

     - или -

   - Раскройте **Белый список**, затем выберите пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, заданное для этого пользователя или группы, а затем выберите команду **Удалить**.

     - или -

   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление**. В левой части диалогового окна **Белый список протоколов** в области **Пользователи** выберите пользователя или группу, для которой задано правило. В правой части диалогового окна **Белый список протоколов** в области **Правила** выберите правило и затем нажмите кнопку **Удалить** или щелкните правой кнопкой мыши правило и затем выберите команду **Удалить**.

Базовый IP-файрвол

IP-файрвол дает контроль над сетевым трафиком, который не охватывается распознаваемыми протоколами или белым списком протоколов, повышая безопасность сетевого взаимодействия. С помощью файрвола можно отслеживать TCP- и UDP-пакеты, запрещать нежелательный трафик, а также блокировать подключения к отдельным узлам независимо от политик доступа, заданных для сетевых протоколов.

IP-файрвол использует набор правил для разрешения или блокирования трафика в сетевом соединении. Каждое правило задает критерий, которому должен соответствовать пакет, а также ответное действие, которое будет выполняться при соответствии правилу (принять или отклонить). Когда клиентский компьютер пытается подключиться к другому компьютеру, файрвол автоматически проверяет входящие и исходящие пакеты в трафике согласно заданному набору правил. Когда первое соответствие будет найдено, файрвол разрешит или заблокирует пакеты.

При помощи правил файрвола можно разрешить только определенные сетевые соединения с учетом направления трафика, протокола, адреса удаленного хоста и портов подключения. Хосты могут быть идентифицированы по адресам IPv4 или IPv6.

Есть два основных подхода к настройке файрвола:

- Можно запретить весь трафик и создать исключения для определенных соединений.
- Можно закрыть доступ к определенным узлам и/или портам.

Под узлом **Протоколы** > **Базовый IP-файрвол** в дереве консоли перечисляются пользователи и группы, для которых заданы правила файрвола. Правила могут быть заданы индивидуально для каждого пользователя и группы.

Контекстное меню базового IP-файрвола содержит следующие команды:

- **Удалить пользователя** - Удаляет пользователя или группу из белого списка.
- **Управление** - Открывает диалоговое окно, позволяющее задать или отредактировать правила файрвола для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее задать или отредактировать правила файрвола для автономного режима.
- **Загрузить** - Позволяет импортировать ранее сохраненный файл с правилами файрвола для оперативного режима.
- **Загрузить офлайновые настройки** - Позволяет импортировать ранее сохраненный файл с правилами файрвола для автономного режима.
- **Сохранить** - Позволяет экспортировать правила файрвола, заданные для оперативного режима, в файл с расширением `.ipp`, который затем можно импортировать и использовать на другом компьютере.
- **Сохранить офлайновые настройки** - Позволяет экспортировать правила файрвола, заданные для автономного режима, в файл с расширением `.ipp`, который затем можно импортировать и использовать на другом компьютере.
- **Сбросить** - Сбрасывает правила файрвола для оперативного режима в состояние “не задано”. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.
- **Сбросить офлайновые настройки** - Сбрасывает правила файрвола для автономного режима в состояние “не задано”. Если правила для автономного режима не заданы, к клиентским компьютерам, находящимся не в сети, применяются правила, заданные для оперативного режима.
- **Удалить офлайновые настройки** - Блокирует наследование правил файрвола, заданных для автономного режима, и принудительно применяет правила, заданные для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

Дополнительные сведения см. в разделе Действия по управлению файрволом.

Правила файрвола

Если выбрать пользователя или группу под узлом **Протоколы** > **Базовый IP-файрвол** в дереве консоли, на панели сведений отображаются правила белого списка, заданные для этого пользователя или группы. Для каждого правила список содержит следующие сведения:

- **Имя** - Имя правила.
- **Подавлять разрешения протоколов** - Показывает, настроено ли данное правило для блокировки доступа к определенным узлам (подробнее см. в описании параметра Подавлять разрешения протоколов).
- **Протокол(ы)** - Протоколы, к которым применяется правило: **TCP** и/или **UDP**.
- **Тип** - Действие файрвола для всех подключений, удовлетворяющих правилу. Возможные варианты: **Разрешено** (разрешает подключение) и **Запрещено** (блокирует подключение).
- **Направление** - Направление трафика, к которому применяется правило: **Входящие** и/или **Исходящие**.
- **Хосты** - Узлы, к которым применяется правило.
- **Порты** - Порты, к которым применяется правило.
- **Отправить алерт** - Показывает, включены ли оповещения для данного правила.
- **Протоколировать событие** - Показывает, включена ли регистрация событий в журнале аудита для данного правила.
- **Профиль** - Возможные значения: **Обычный** и **Офлайн**. Значение **Обычный** указывает, что правило применяется к клиентским компьютерам, находящимся в сети. Значение **Офлайн** указывает, что правило применяется к клиентским компьютерам, работающим автономно.

  Можно задавать правила файрвола для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Для получения информации о том, как задать настройки безопасности для автономного режима, см. раздел Управление базовым IP-файрволом для автономного режима.

Контекстное меню правила в списке на панели сведений содержит следующие команды:

- **Управление** - В зависимости от профиля данного правила (обычный или офлайн), открывает диалоговое окно, в котором можно задать правила файрвола для оперативного или автономного режима.
- **Редактировать** - Открывает диалоговое окно, в котором можно просмотреть или изменить правило файрвола.
- **Отправить алерт** - Включает или отключает отправку оповещений для данного правила.
- **Протоколировать событие** - Включает или отключает протоколирование событий для данного правила.
- **Удалить** - Удаляет данное правило.

Дополнительные сведения см. в разделе Действия по управлению файрволом.

Параметры правил файрвола

Параметры правил файрвола задают условия разрешения или блокирования сетевого соединения. У правила имеются следующие параметры:

- Имя
- Подавлять разрешения протоколов
- Протокол
- Тип
- Направление
- Если правило срабатывает
- Хосты
- Порты

Имя

Параметр **Имя** задает имя, позволяющее идентифицировать правило.

Подавлять разрешения протоколов

Если установлен флажок **Подавлять разрешения протоколов**, правило блокирует доступ к узлам, указанным в параметре Хосты. Такое правило запрещает любые подключения к этим узлам независимо от разрешений, настроенных для протоколов. В результате пользователь не может получить доступ к узлу, даже если доступ разрешен на уровне протокола (см. Разрешения на доступ к протоколам).

Установка этого флажка влияет на следующие настройки правила:

- **Протокол** - Выбраны протоколы TCP и UDP. Правило реагирует как на TCP-, так и на UDP-подключения.
- **Тип** - Выбран тип Запрет. Правило служит для запрета подключений.
- **Направление** - Выбраны оба направления. Правило запрещает как входящие, так и исходящие подключения.
- **Порт** - Настройка недоступна. Правило запрещает подключения через любой порт TCP или UDP.

Внимание: Если установлен флажок **Подавлять разрешения протоколов**, то звездочка с точкой (`*.`) в параметре Хосты соответствует не только произвольной последовательности символов, которая заканчивается точкой, но и отсутствию символов (в том числе точки). Так, правило с именем узла `*.host.com` заблокирует доступ к `www.host.com` и `host.com`. Чтобы заблокировать доступ только к узлу `host.com`, необходимо указать именно это имя, `host.com`. Доступ к `www.host.com` в таком случае не блокируется.

Протокол

Параметр **Протокол** задает протокол, по которому передаются пакеты. Возможные варианты: **TCP** и **UDP**.

Тип

Параметр **Тип** определяет действие применительно к IP-трафику, который соответствует условиям правила. Можно выбрать одно из следующих действий:

- **Разрешение** - Беспрепятственно пропускать IP-трафик.
- **Запрет** - Блокировать IP-трафик сразу после начала передачи данных.

Направление

Параметр **Направление** задает направление трафика, к которому применяется правило. Возможные варианты:

- **Входящие** - Правило применяется к входящему трафику.
- **Исходящие** - Правило применяется к исходящему трафику.

Если правило срабатывает

Параметр **Если правило срабатывает** задает следующие дополнительные операции, которые будут выполняться при срабатывании правила:

- **Отправить алерт** - При каждом срабатывании правила рассылается тревожное оповещение. DeviceLock рассылает тревожные оповещения с учетом соответствующих настроек. В этих настройках задается адресат и способ отправки оповещений. Перед включением оповещений для правила файрвола задайте параметры оповещений в настройках сервиса DeviceLock (см. раздел Алерты).
- **Протоколировать событие** - Событие регистрируется в журнале аудита при каждом срабатывании правила.

Просмотрщик журнала аудита отобразит следующую информацию о событии:

- **Тип** - `Успех` в случае разрешенного доступа, `Отказ` в случае запрещенного доступа.
- **Дата/Время** - Дата и время создания соединения в следующем формате: дд.мм.гггг чч:мм:сс. Пример: `05.06.2012 14:54:46`. Для разрешенного трафика - дата и время создания соединения. Для запрещенного трафика - дата и время отклонения пакета.
- **Источник** - Тип протокола: `IP`
- **Действие** - Тип пользовательского действия: `Входящее соединение` либо `Исходящее соединение`
- **Имя** - Пустое поле.
- **Информация** - IP-адрес, номер порта и полное доменное имя (FQDN) удаленного узла. Пример:
  `Удаленный хост: 192.168.100.10:99 (mycomputer.mygroup.mydomain.com)`
- **Причина** - Причина возникновения события: `Базовый IP-файрвол: “<имя_правила>”`
- **Пользователь** - Имя пользователя, связанного с данным событием, в следующем формате: <имя_домена>\<имя_пользователя>.
- **PID** - Идентификатор процесса приложения, связанного с событием. Пример: `4420`
- **Процесс** - Полный путь к исполняемому файлу процесса. Пример:
  `C:\Program Files\AppFolder\AppName.exe`

Хосты

Параметр **Хосты** задает удаленные узлы (компьютеры, серверы, веб-сайты и т.п.), к которым применяется правило.

Узлы можно указать в любом из следующих форматов:

- DNS-имя или URI ресурса (например, `www.host.com` или `wwww.host.com/path/resource`). Для обозначения произвольной группы символов в DNS-имени или URI ресурса можно использовать звездочку (например, `*.host.com` соответствует любому имени, которое заканчивается на `.host.com`).

  Внимание: Если установлен флажок Подавлять разрешения протоколов, то звездочка с точкой (`*.`) в DNS-имени или URI ресурса соответствует не только произвольной последовательности символов, которая заканчивается точкой, но и отсутствию символов, в том числе точки. Так, правило с именем узла `*.host.com` заблокирует доступ к `www.host.com` и `host.com`. Чтобы заблокировать доступ только к узлу `host.com`, необходимо указать именно это имя, `host.com`. Доступ к `www.host.com` в таком случае не блокируется.

- IPv4-адрес (например, `12.13.14.15`). Можно указывать диапазон IPv4-адресов, разделенных дефисом (-) (например, `12.13.14.18-12.13.14.28`).
- IPv6-адрес, например `fe80:0000:0000:0000:0a2f:7e00:0004:533a`, `fe80:0:0:0:a2f:7e00:4:533a` или `fe80::a2f:7e00:4:533a`.

Чтобы указать несколько узлов, их можно разделять запятой (,) или точкой с запятой (;), или нажимать клавишу ENTER после ввода каждой строчки. Узлы можно указывать в различных форматах, описанных выше (например, `www.microsoft.com; 12.13.14.15, 12.13.14.18-12.13.14.28`).

Примечание: Если указать узлы, не задав порты, правило будет разрешать или блокировать все клиентские подключения к указанным узлам.

Порты

Параметр **Порты** задает порты на удаленных узлах, к которым применяется правило. Можно указать отдельный порт или диапазон портов, разделенных дефисом (-). Например, чтобы открыть порт 110, укажите `110`. Чтобы открыть порты с 5000 по 5020 включительно, укажите `5000-5020`. Чтобы указать несколько портов, их можно разделять запятой (,) или точкой с запятой (;). Например `110, 36; 8080, 5000-5020`. Также можно нажимать клавишу ENTER после ввода каждой строчки.

Примечание: Если указать порты, не задав узлы, правило будет разрешать или блокировать все клиентские подключения к указанным портам.

Действия по управлению файрволом

Управление файрволом для оперативного режима предполагает:

- Создание правил файрвола
- Редактирование правил файрвола
- Копирование правил файрвола
- Экспорт и импорт правил файрвола
- Сброс правил файрвола в исходное состояние
- Удаление правил файрвола

Для управления правилами файрвола можно использовать консоль DeviceLock Management Console, DeviceLock Group Policy Manager или DeviceLock Service Settings Editor.

Примечание: Можно задавать разные правила для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Правила оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Правила автономного режима (офлайн-профиль) применяются при автономной работе клиентских компьютеров. По умолчанию правила автономного режима используются, если у клиентского компьютера отключен сетевой кабель. Подробнее об автономном режиме см. в разделе Политики безопасности DeviceLock (офлайн-профиль). Инструкции по настройке правил автономного режима, см. в разделе Управление базовым IP-файрволом для автономного режима.

Создание правил файрвола

При настройке правил файрвола необходимо учитывать следующее:

- Если для некоторого пользователя или группы пользователей одновременно заданы правила, разрешающие и запрещающие определенный протокол, то разрешающие правила имеют приоритет как для входящего, так и для исходящего трафика.
- Разрешения протоколов имеют более высокий приоритет по сравнению с правилами файрвола, за исключением правил с включенным параметром Подавлять разрешения протоколов, блокирующих доступ даже при наличии разрешений.

  Внимание: Правила с включенным параметром Подавлять разрешения протоколов не блокируют доступ, разрешенный правилами белого списка для протоколов Любой и/или SSL. Они также не блокируют доступ по протоколам, которые не распознаются в NetworkLock, если доступ разрешен другими правилами файрвола.

- Некоторые приложения (например, стандартные программы Windows, такие как “Удаленный рабочий стол”) передают данные через системные процессы. Чтобы заблокировать такие приложения, создайте и примените правило файрвола к учетной записи, которую использует процесс приложения, передающий данные.
- Когда пользователь пытается установить соединение, которое ему не разрешено, выводится сообщение о блокировании от IP-файрвола, если соответствующий параметр включен настройках сервиса DeviceLock (см. описание параметра Сообщение о блокировании от IP-файрвола.
- Взаимодействие между сервисом DeviceLock и сервером DeviceLock Enterprise Server, а также между сервисом DeviceLock и консолью DeviceLock Management Console всегда разрешено независимо от настроек файрвола.
- Можно включить тревожные оповещения о том, что сработало какое-либо правило файрвола. Такие оповещения включаются при настройке правила.

  Тревожные оповещения рассылаются в соответствии с параметрами сервиса DeviceLock, задающими адресата и способ доставки оповещений. Перед включением оповещений необходимо настроить соответствующие параметры сервиса (см. раздел Алерты).

Чтобы создать правило файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

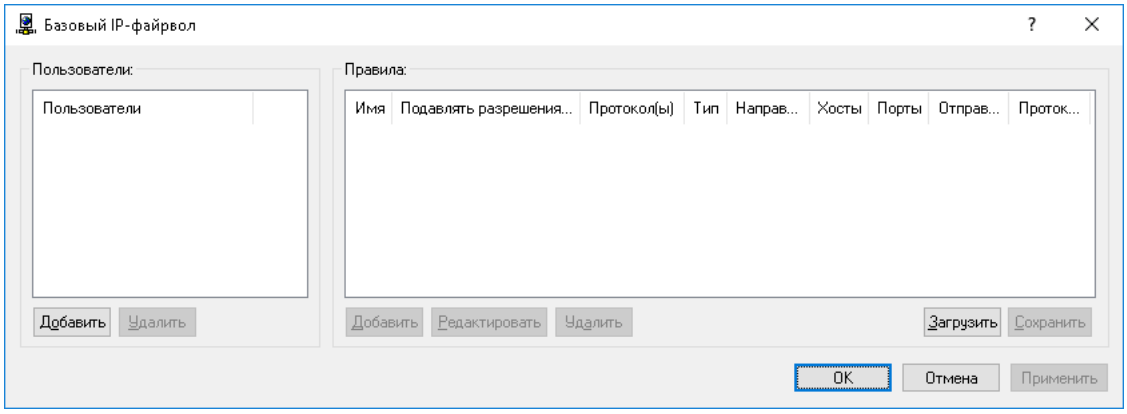
3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление**.

     - или -

   - Выберите **Базовый IP-файрвол**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно "Базовый IP-файрвол".



4. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно Выбор: ""Пользователи" или "Группы"".

5. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать правило файрвола, и нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области "Пользователи" в левой части диалогового окна "Базовый IP-файрвол".

   Чтобы удалить пользователя или группу, в левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи**, выберите пользователя или группу, а затем нажмите кнопку **Удалить**.

6. В области **Пользователи** диалогового окна **Базовый IP-файрвол** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

7. В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** нажмите кнопку **Добавить**.

   Появится диалоговое окно "Добавить правило".

8. В диалоговом окне **Добавить правило** задайте параметры правила:

   - Чтобы задать имя правила, введите его в поле **Имя**.
   - Чтобы блокировать доступ к узлам, указанным в параметре **Хосты**, установите флажок **Override Protocols Permissions**. Подробнее см. в описании параметра Подавлять разрешения протоколов.
   - Чтобы указать протокол, в разделе **Протокол** установите флажок рядом с требуемым протоколом. Подробнее см. в описании параметра Протокол.
   - Чтобы указать действия, которые файрвол должен выполнять для всех подключений, удовлетворяющих правилу, в области **Тип** выберите один из следующих вариантов: **Разрешение** или **Запрет**. Подробнее см. в описании параметра Тип.
   - Чтобы указать направление трафика, к которому применяется правило, в области **Направление** установите соответствующий флажок. Подробнее см. в описании параметра Направление.
   - Чтобы указать дополнительные действия, которые будут выполняться при срабатывании правила, в области **Если правило срабатывает** установите соответствующий флажок. Подробнее см. в описании параметра Если правило срабатывает.
   - Чтобы указать удаленные узлы, к которым применяется правило, в поле **Хосты** введите имена узлов или их IP-адреса через запятую или точку с запятой. Подробнее см. в описании параметра Хосты.
   - Чтобы указать порты удаленных узлов, к которым применяется правило, в поле **Порты** введите номера портов через запятую или точку с запятой. Подробнее см. в описании параметра Порты.

9. Нажмите кнопку **OK**.

   Созданное правило появится в области "Правила" в правой части диалогового окна "Базовый IP-файрвол".

10. Нажмите кнопку **OK** или **Применить**.

    Пользователи и группы, для которых заданы правила файрвола, отображаются в дереве консоли в узле "Базовый IP-файрвол".

Если в дереве консоли выбрать пользователя или группу, для которой задано правило файрвола, на панели сведений отобразится информация о заданном правиле (подробнее см. в разделе Правила файрвола).

Редактирование правил файрвола

Можно изменять значения параметров, настроенных для правила файрвола, в любое время.

Чтобы изменить правило файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.
   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте **Протоколы**.
3. В узле **Протоколы** щелкните правой кнопкой мыши **Базовый IP-файрвол**, выберите команду **Управление**, а затем выполните следующие действия:
   a) В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** выберите пользователя или группу, для которого требуется изменить правило.

      Если выбрать пользователей или группы, в области "Правила" в правой части диалогового окна отобразятся правила файрвола, которые применяются к этим пользователям или группам.
   b) В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** выберите правило, которое требуется редактировать, а затем нажмите кнопку **Редактировать**.

      - или -

      Щелкните правой кнопкой мыши правило, а затем выберите команду **Редактировать**.

   - или -

   В узле **Протоколы** раскройте узел **Базовый IP-файрвол** и выполните следующее:
   a) В узле **Базовый IP-файрвол** выберите пользователя или группу, для которой необходимо изменить правило.

      Если выбрать пользователей или группы, на панели сведений отобразятся правила файрвола, которые применяются к этим пользователям или группам.
   b) На панели сведений щелкните правой кнопкой мыши правило, которое требуется редактировать, а затем выберите команду **Редактировать**.

      - или -

      На панели сведений дважды щелкните правило, которое требуется редактировать.
4. В диалоговом окне **Редактирование правила** внесите необходимые изменения.
5. Нажмите кнопку **OK**, чтобы применить изменения.

Копирование правил файрвола

Можно выполнять операции вырезать-вставить, копировать-вставить, а также операции перетаскивания, чтобы повторно использовать существующие правила файрвола.

Чтобы скопировать правило файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление**.

     - или -

   - Выберите **Базовый IP-файрвол**, а затем щелкните значок **Управление** на панели инструментов.

   Появится диалоговое окно "Базовый IP-файрвол".

4. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** выберите пользователя или группу, к которой применяется правило, которое требуется скопировать.

   Если выбрать пользователей или группы, в области "Правила" в правой части диалогового окна отобразятся правила файрвола, которые применяются к этим пользователям или группам.

5. В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** щелкните правой кнопкой мыши правило, которое требуется скопировать, а затем выберите команду **Копировать** или **Вырезать**.

   Вырезанное или скопированное правило автоматически копируется в буфер обмена.

   Также можно использовать сочетания клавиш CTRL+C, CTRL+X и CTRL+V, чтобы скопировать, вырезать и вставить правило. При нажатии CTRL+X правило будет вырезано только после того, как вы его вставите.

   Можно одновременно скопировать и вставить сразу несколько правил. Для этого удерживая клавишу SHIFT или CTRL, последовательно выберите каждое правило, затем щелкните их правой кнопкой мыши и выберите **Копировать**.

6. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

7. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых должно применяться скопированное правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой части диалогового окна “Базовый IP-файрвол”.

8. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** выберите пользователей или группы, для которых требуется задать скопированное правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

9. В правой части диалогового окна **Базовый IP-файрвол** щелкните правой кнопкой мыши в области **Правила**, а затем выберите команду **Вставить**.

   Скопированное правило появится в области “Правила” в правой части диалогового окна “Базовый IP-файрвол”.

10. Нажмите кнопку **OK** или **Применить**, чтобы применить скопированное правило.

Экспорт и импорт правил файрвола

Можно экспортировать все заданные правила файрвола в файл с расширением `.ipp`, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт правил также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать правила файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Сохранить**.

     - или -
   - Выберите **Базовый IP-файрвол**, а затем щелкните значок **Сохранить** на панели инструментов.

     - или -
   - Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Сохранить**.

     - или -
   - Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши любого пользователя или группу в правиле файрвола. На панели сведений щелкните правой кнопкой правило файрвола, а затем выберите команду **Сохранить**.

     - или -
   - Раскройте **Базовый IP-файрвол**, выберите любого пользователя или группу в правиле файрвола, а затем щелкните **Сохранить** на панели инструментов.

     - или -
   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление.** В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** нажмите кнопку **Сохранить**.
4. В появившемся диалоговом окне выберите папку, в которую требуется сохранить файл, задайте имя файла, и нажмите кнопку **Сохранить**.

   При экспорте правила сохраняются в файле с расширением .ipp.

Чтобы импортировать правила файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Загрузить**.

     - или -
   - Выберите **Базовый IP-файрвол**, а затем щелкните значок **Загрузить** на панели инструментов.

     - или -

- Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Загрузить**.

  - или -

- Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши любого пользователя или группу в правиле файрвола. На панели сведений щелкните правой кнопкой правило файрвола, а затем выберите команду **Загрузить**.

  - или -

- Раскройте **Базовый IP-файрвол**, выберите любого пользователя или группу в правиле файрвола, а затем щелкните **Загрузить** на панели инструментов.

  - или -

- Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление.** В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** нажмите кнопку **Загрузить**.

4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

   Если правила файрвола уже настроены и вы импортируете новые правила, появится следующее сообщение: "Вы хотите перезаписать существующие записи (Да - перезаписать, Нет - добавить)?" В окне сообщения нажмите кнопку "Да", чтобы перезаписать существующие правила файрвола. Нажмите кнопку "Нет", чтобы добавить новые правила файрвола к существующим.

Сброс правил файрвола в исходное состояние

Если для развертывания политик DeviceLock используется DeviceLock Group Policy Manager или DeviceLock Service Settings Editor, могут возникнуть ситуации, когда потребуется отменить применение заданных правил файрвола к определенной группе компьютеров. Для этого необходимо вернуть ранее заданные правила в исходное "неопределенное" состояние. Все параметры сервиса DeviceLock, которые установлены в состояние "не определен", игнорируются на клиентских компьютерах.

Чтобы сбросить правила файрвола в исходное состояние

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Сбросить**.

Удаление правил файрвола

Можно удалить правила файрвола, если они больше не нужны.

Чтобы удалить правило файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши пользователя или группу, для которой задано правило, а затем выберите команду **Удалить пользователя**.

     Если удалить пользователя или группу, все правила, заданные для этого пользователя или группы, автоматически удалятся.

     - или -

   - Раскройте **Базовый IP-файрвол**, затем выберите пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, заданное для этого пользователя или группы, а затем выберите команду **Удалить**.

     - или -

   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление.** В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** выберите пользователя или группу, для которой задано правило. В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** выберите правило и затем нажмите кнопку **Удалить** или щелкните правой кнопкой мыши правило и затем выберите команду **Удалить**.

Настройки безопасности для протоколов

Используя узел **Протоколы** > **Настройки безопасности**, можно включить дополнительные параметры безопасности, которые влияют на установленные разрешения и правила аудита для протоколов. Описание этих параметров см. в разделе Описание настроек безопасности.

Контекстное меню узла **Настройки безопасности** содержит следующие команды:

- **Управление** - Открывает диалоговое окно, позволяющее совместно включать или отключать настройки безопасности для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее совместно включать или отключать настройки безопасности для автономного режима.

Если в дереве консоли выбран узел **Настройки безопасности**, на панели сведений отображается список настроек. Чтобы управлять настройкой, щелкните ее правой кнопкой мыши на панели сведений и используйте команды контекстного меню:

- **Включить** - Включает настройку безопасности для оперативного режима.
- **Выключить** - Отключает настройку безопасности для оперативного режима.
- **Сбросить** - Сбрасывает настройку для оперативного режима в состояние “не задано”. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.
- **Включить офлайн** - Включает настройку безопасности для автономного режима.
- **Выключить офлайн** - Отключает настройку безопасности для автономного режима.
- **Сбросить офлайновые настройки** - Сбрасывает все ранее заданные настройки для автономного режима в состояние “не задано”. Если настройки безопасности для автономного режима не заданы, к клиентским компьютерам, находящимся не в сети, применяются настройки безопасности для оперативного режима.
- **Управление** - Открывает диалоговое окно, позволяющее совместно включать или отключать настройки безопасности для оперативного режима.
- **Управление офлайновыми настройками** - Открывает диалоговое окно, позволяющее совместно включать или отключать настройки безопасности для автономного режима.
- **Удалить офлайновые настройки** - Блокирует наследование настроек безопасности для автономного режима и принудительно применяет настройки, заданные для оперативного режима. Эта команда доступна только в DeviceLock Group Policy Manager и DeviceLock Service Settings Editor.

Чтобы изменить настройки оперативного режима (обычный профиль), можно дважды щелкнуть соответствующую настройку на панели сведений для изменения ее состояния (**Включено** / **Отключено**). Также можно щелкнуть настройку правой кнопкой мыши и выбрать пункт **Управление** в контекстном меню, или нажать соответствующую кнопку на панели инструментов.

Дополнительные сведения см. в разделе Действия по управлению настройками безопасности.

Описание настроек безопасности

DeviceLock предоставляет следующие настройки безопасности для протоколов:

- **Блокировать нераспознанный исходящий SSL-трафик** - Если включено, то сервис DeviceLock проводит аудит и блокирует весь нераспознанный исходящий SSL-трафик. Если настройка отключена, то даже при заблокированных протоколах нераспознанный исходящий SSL-трафик не блокируется и аудит для него не выполняется.
- **Блокировать URL, содержащие IP-адреса** - Если включено, то сервис DeviceLock блокирует соединения по любым URL, содержащим IP-адрес, даже если пользователю разрешено использовать протокол. Данная настройка влияет на все протоколы, кроме следующих: FTP, IBM Notes, IRC, Jabber, MAPI, SMB, SMTP, Telnet и Торрент. По умолчанию она отключена.

  Применительно к протоколам, на которые влияет данная настройка, контроль доступа, аудит и теневое копирование для URL, содержащих IP-адрес, выполняются на уровне протокола HTTP. При запрете доступа по протоколу HTTP соединения с использованием содержащих IP-адрес URL блокируются для всех таких протоколов, даже если настройка **Блокировать URL, содержащие IP-адреса** не включена.

  Внимание: Если белый список протоколов разрешает доступ по протоколу Любой к определенным IP-адресам, настройка **Блокировать URL, содержащие IP-адреса** не будет блокировать соединения с этими IP-адресами.

- **Блокировать прокси трафик** - Если включено, то сервис DeviceLock регистрирует и блокирует весь трафик, идущий через прокси-сервер. Поддерживаются следующие типы прокси-серверов: HTTP, SOCKS4 и SOCKS5.
- **Блокировать сеть, если служба BFE остановлена (для Windows 8 и выше)** - Если включено, то сервис DeviceLock блокирует весь сетевой трафик при остановленной системной службе базовой фильтрации (BFE). Если эта настройка отключена и служба базовой фильтрации остановлена, модуль NetworkLock не сможет контролировать сетевой трафик на компьютерах под управлением ОС Windows 8 и более поздних версий. Для включения данной настройки необходимо, чтобы была задана политика NetworkLock (любые связанные с протоколами разрешения или правила сервиса DeviceLock). В противном случае эта настройка не действует.
- **Перехватывать соединения MS Lync** - Если включено, позволяет сервису DeviceLock перехватывать сетевой трафик приложения Microsoft Lync 2010 или Microsoft Office Communicator. Для включения данной настройки необходимо, чтобы была задана политика NetworkLock (любые связанные с протоколами разрешения или правила сервиса DeviceLock). В противном случае эта настройка не действует.
- **Блокировать трафик Tor-браузера** - Если включено, то сервис DeviceLock блокирует подключение к сети Tor, предотвращая использование Tor-браузера. Для включения данной настройки необходимо, чтобы была задана политика NetworkLock (любые связанные с протоколами разрешения или правила сервиса DeviceLock). В противном случае эта настройка не действует.

  Когда действует эта настройка, попытки использовать Tor-браузер регистрируются в журнале аудита как события запрета подключения, где в качестве источника указан Tor-браузер, и учитываются как запрещенные попытки доступа к протоколу Другие (Other) в отчетах по данным журнала аудита (отчеты категории Audit Log).

- **Перехватывать черновики MAPI-сообщений** - Если включено, то сервис DeviceLock контролирует папку черновиков, сохраняемых приложением Outlook на сервере Exchange. Когда включена эта настройка, все правила и разрешения DeviceLock, заданные для протокола MAPI, применяются к таким черновикам. Отключите эту настройку, если не требуется, чтобы DeviceLock контролировал черновики сообщений.
- **Перехватывать перемещенные MAPI-сообщения** - Если включено, то сервис DeviceLock контролирует сообщения, импортируемые на сервер Exchange из внешних файлов почтовых сообщений (.msg-файлов) или других (внешних) почтовых ящиков. Когда включена эта настройка, все правила и разрешения DeviceLock, заданные для протокола MAPI, применяются к сообщениям из .msg-файлов или внешних почтовых ящиков, отправляемым на сервер Exchange приложением Outlook. Отключите эту настройку, если не требуется, чтобы DeviceLock контролировал такие сообщения.

Действия по управлению настройками безопасности

Управление настройками безопасности для протоколов для оперативного режима предполагает:

- Задание и редактирование настроек безопасности
- Сброс настроек безопасности в исходное состояние

Примечание: Можно задавать настройки безопасности для разных режимов работы (оперативного и автономного). Настройки безопасности для оперативного режима (обычный профиль) применяются, когда клиентские компьютеры находятся в сети. Настройки безопасности для автономного режима (офлайн-профиль) применяются, когда клиентские компьютеры работают автономно. По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру. Для получения дополнительной информации о политиках DeviceLock для автономного режима работы см. раздел Политики безопасности DeviceLock (офлайн-профиль). Для получения информации о том, как задать настройки безопасности для автономного режима, см. раздел Управление настройками безопасности для автономного режима.

Настройки безопасности для протоколов для оперативного режима могут иметь одно из следующих состояний:

- **Не задано** - Показывает, что настройки безопасности не заданы для протоколов.
- **Включено** - Показывает, что настройки безопасности включены для протоколов.
- **Отключено** - Показывает, что настройки безопасности отключены для протоколов.

Задание и редактирование настроек безопасности

Чтобы задать и редактировать настройки безопасности

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

a) Откройте Group Policy Object Editor.

b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

- Выберите **Настройки безопасности**. На панели сведений щелкните правой кнопкой мыши нужную настройку безопасности, а затем выберите команду **Включить** или **Выключить**.

  - или -

- Щелкните правой кнопкой мыши **Настройки безопасности**, а затем выберите команду **Управление.** В открывшемся диалоговом окне установите флажки для настроек, которые требуется включить, а затем нажмите кнопку **OK**.

  Другой способ открыть это окно - выбрать "Настройки безопасности" в дереве консоли, а затем щелкнуть значок "Управление" на панели инструментов.

Сброс настроек безопасности в исходное состояние

Если для развертывания политик DeviceLock используется DeviceLock Group Policy Manager или DeviceLock Service Settings Editor, могут возникнуть ситуации, когда требуется отменить применение заданных настроек безопасности для протоколов к определенной группе компьютеров. Для этого необходимо вернуть ранее заданные настройки безопасности в исходное "неопределенное" состояние. Все параметры сервиса DeviceLock, которые установлены в состояние "не определен", игнорируются на клиентских компьютерах.

Чтобы сбросить настройки безопасности в исходное "неопределенное" состояние

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера** > **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выберите **Настройки безопасности**.

   На панели сведений отобразятся настройки безопасности.

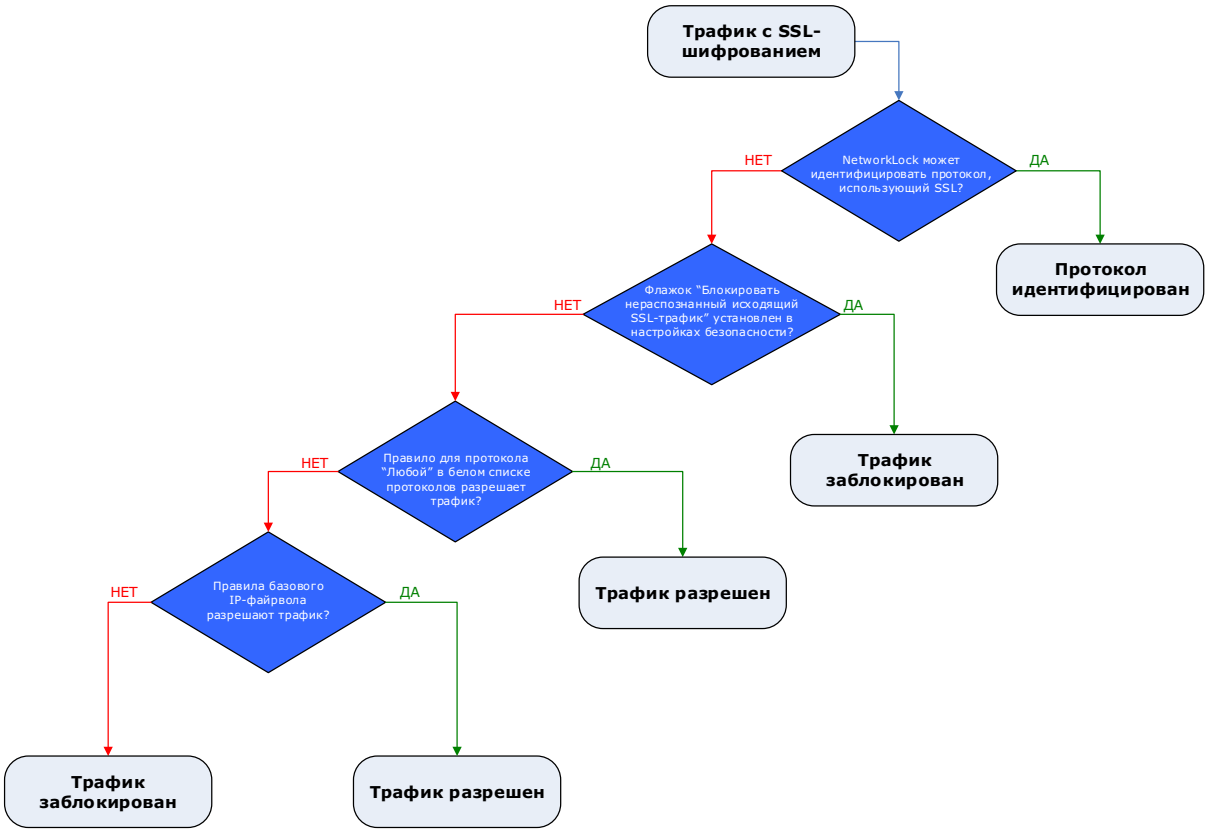
4. На панели сведений щелкните правой кнопкой мыши нужную настройку безопасности, а затем выберите команду **Сбросить**.

Контроль трафика с SSL-шифрованием

Контроль трафика с SSL-шифрованием включает в себя следующие последовательно выполняемые операции:

1. Идентификацию протокола, использующего SSL. После идентификации протокола DeviceLock проверяет, есть ли у пользователя разрешение на запрошенное им подключение (см. диаграмму в разделе Управляемый контроль доступа).
2. Проверку того, установлен ли параметр Блокировать нераспознанный исходящий SSL-трафик (см. раздел Настройки безопасности для протоколов).
3. Проверку того, разрешен ли трафик правилом из белого списка для протокола **Любой** (см. описание параметра Протокол в разделе Белый список протоколов).
4. Проверку того, разрешен ли трафик правилом файрвола.

Ниже на примере показано, как DeviceLock проверяет трафик с SSL-шифрованием и применяет соответствующие меры безопасности с учетом заданных политик.



8

Политики безопасности DeviceLock (офлайн-профиль)

В этой главе:

Общая информация

Настройка конфигурации для автономного режима

Переключение между оперативным и автономным режимами

Управление политиками безопасности для автономного режима (устройства)

Управление политиками безопасности для автономного режима (протоколы)

Общая информация

В современных условиях во многих компаниях есть пользователи, использующие корпоративные служебные данные, когда сетевое подключение отсутствует. Например, торговые представители, страховые агенты и региональные инспекторы, находясь в рабочих поездках, все чаще работают на корпоративных портативных компьютерах вне сети. Защита конфиденциальной информации на таких мобильных компьютерах является одним из основных приоритетов для многих организаций.

DeviceLock обеспечивает надежную защиту уязвимых корпоративных данных при отсутствии доступа к корпоративной среде. Можно контролировать доступ пользователей к устройствам и протоколам, а также обеспечить теневое копирование данных, записанных или переданных пользователем по сети, в различных сценариях автономной работы. DeviceLock также обеспечивает большую гибкость управления, т.к. позволяет настраивать политики безопасности для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп.

Политики для оперативного режима применяются для пользователей, когда клиентский компьютер подключен к корпоративной сети, или к указанным серверам DeviceLock Enterprise Server, или к контроллеру домена Active Directory. Политики для автономного режима применяются для пользователей, когда клиентский компьютер отключен от корпоративной сети, или от указанных серверов DeviceLock Enterprise Server, или от контроллера домена Active Directory.

Чтобы настроить применение разных политик DeviceLock для оперативного и автономного режимов работы, необходимо задать настройки соответствующих профилей:

- **Обычный профиль** - Настройки этого профиля применяются на компьютерах, находящихся в сети.
- **Офлайн-профиль** - Настройки этого профиля применяются на компьютерах, работающих автономно (например, когда пользователи во время рабочих поездок используют корпоративные компьютеры вне сети).

Если настройки офлайн-профиля не заданы, в автономном режиме применяются настройки обычного профиля.

Различные настройки каждого из этих профилей можно задать для параметров “Разрешения”, “Аудит, Теневое копирование и Алерты”, “Белый список USB-устройств”, “Белый список носителей”, “Белый список” (для протоколов), “Контентно-зависимые правила”, “Базовый IP-файрвол” и “Настройки безопасности”. Управлять настройками офлайн-профиля можно из консоли DeviceLock Management Console, DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

В следующих сценариях представлены примеры использования разных политик DeviceLock для оперативного и автономного режима работы в целях обеспечения лучшей защиты корпоративных данных.

- **Сценарий 1.** Предположим, в организации есть группа пользователей “Финансы”. Как администратор, вы можете предоставить членам этой группы доступ на запись файлов на следующие устройства: “Съемные устройства”, “Оптический привод”, “USB-порт” и “Гибкий диск”, когда они находятся в оперативном режиме (в сети). При этом действия пользователей в сети будут регистрироваться в журнале аудита, любые скопированные файлы будут сохраняться в журнале теневого копирования; журналы аудита и теневого копирования будут посылаться на сервер DeviceLock Enterprise Server. В автономном режиме работы пользователям группы “Финансы” будет запрещен доступ на запись файлов.

  Такие политики безопасности позволяют контролировать действия пользователей группы “Финансы” в режиме реального времени. Анализируя данные журналов аудита и теневого копирования на сервере DeviceLock Enterprise Server, вы можете надлежащим образом и своевременно отреагировать на появление угрозы утечки данных. Пользователь не сможет воспользоваться временным отключением компьютера от сети, чтобы за это время скопировать важные данные на устройство, избежать отправки теневых копий на сервер DeviceLock Enterprise Server и, таким образом, скрыть от службы безопасности кражу данных.

- **Сценарий 2.** Представьте себе пользователя по имени Мария, торгового представителя крупной компании, имеющую портативный компьютер и часто работающую вне офиса. Ей необходимо предоставлять бизнес-партнерам файлы с результатами ее работы. В этой ситуации вы можете предоставить Марии доступ на запись определенных файлов на следующие устройства: “Съемные устройства”, “Оптический привод”, “USB-порт” и “Гибкий диск”, и при этом включить теневое копирование для автономного режима работы. В оперативном режиме работы Марии будет запрещен доступ на запись файлов.

  Такие политики безопасности обеспечат большую гибкость в управлении учетными записями пользователей внутри организации, в то же время повышая уровень безопасности корпоративных данных.

Настройка конфигурации для автономного режима

Можно указать сетевые характеристики, которые DeviceLock будет использовать для проверки текущего состояния сетевого подключения (подключен или отключен). По умолчанию DeviceLock работает в автономном режиме, когда сетевой кабель не подключен к клиентскому компьютеру.

Чтобы настроить конфигурацию для автономного режима

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.

2. Выберите узел **Настройки сервиса**.

   Если в дереве консоли выбрать "Настройки сервиса", на панели сведений отобразятся параметры сервиса DeviceLock.

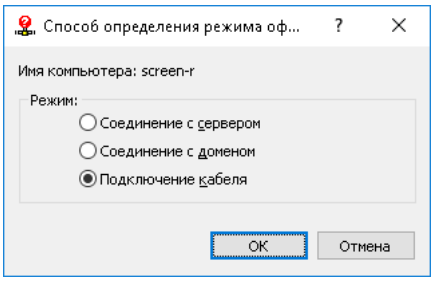
3. На панели сведений выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши параметр **Способ определения режима офлайн**, а затем выберите команду **Свойства**.

     - или -

   - Дважды щелкните **Способ определения режима офлайн**.

   Появится диалоговое окно "Способ определения режима офлайн".



4. В диалоговом окне **Способ определения режима офлайн** выберите любой из следующих вариантов:

   - **Соединение с сервером** - Состояние подключения определяется тем, можно ли передать журналы сервиса DeviceLock с клиентского компьютера на сервер DeviceLock Enterprise Server.

     Считается, что компьютер работает в оперативном режиме, если сервер может получать журналы DeviceLock хотя бы для одного пользователя, использующего этот компьютер в данный момент. Сервер определяется параметром DeviceLock Enterprise Server(ы) в настройках сервиса DeviceLock (см. Настройки сервиса).

     Компьютер считается работающим в автономном режиме, если сервер не в состоянии получить журналы DeviceLock ни для одного из пользователей, которые в данный момент используют этот компьютер. Это может произойти из-за того, что сервису DeviceLock не удается пройти проверку подлинности ни на одном из назначенных серверов DeviceLock Enterprise Server, или все назначенные серверы недоступны.

     Полезный совет: Самый надежный способ обеспечить безопасное соединение - проверка подлинности клиента и сервера на основе сертификата DeviceLock. В этом случае открытый ключ должен быть установлен на клиентских компьютерах, а секретный (закрытый) ключ - на сервере DeviceLock Enterprise Server.

     Если открытый ключ сертификата установлен только на клиентских компьютерах, сервер будет отклонять соединения и клиентские компьютеры будут работать в автономном режиме. Если установить секретный ключ сертификата только на сервере DeviceLock Enterprise Server, то и клиент, и сервер пройдут проверку подлинности, как только соединение будет установлено. Однако такая проверка менее безопасна, чем основанная на сертификате проверка подлинности клиента и сервера. Подробнее о сертификатах DeviceLock см. в разделе Сертификаты DeviceLock.

   - **Соединение с доменом** - Состояние подключения определяется наличием соединения с контроллером домена Active Directory, в который входит данный клиентский компьютер.

     Считается, что компьютер работает в оперативном режиме, если он подключен к контроллеру своего домена. Компьютер считается работающим в автономном режиме, если он не может подключиться ни к одному контроллеру своего домена.

     Если выбран вариант "Соединение с доменом", компьютеры, не включенные в домен (члены рабочей группы или изолированные компьютеры), всегда работают в автономном режиме.

   - **Подключение кабеля** - Состояние подключения определяется тем, подключен ли сетевой кабель к сетевой карте клиентского компьютера. Это простейший и наименее безопасный способ определить состояние сетевого подключения.

     Считается, что компьютер работает в оперативном режиме, если сетевой кабель подключен к его сетевой карте. Компьютер считается работающим в автономном режиме, если сетевой кабель отключен. Обратите внимание, что учитывается только подключение с помощью кабеля. Беспроводные подключения (Wi-Fi и т.п.) и модемные подключения не учитываются.

     Этот вариант выбран по умолчанию.

5. Нажмите кнопку **OK**.

Переключение между оперативным и автономным режимами

Сервис DeviceLock, запущенный на клиентских компьютерах, автоматически определяет состояние подключения к сети и незаметно переключается между оперативным и автономным режимами каждый час и когда происходит одно из следующих событий:

- Пользователь включает компьютер, на котором установлен сервис DeviceLock.

  Сервис DeviceLock всегда запускается в автономном режиме.

- Пользователь входит в систему.
- Пользователь щелкает правой кнопкой мыши значок DeviceLock в области уведомлений панели задач, а затем выбирает команду **Обновить текущее состояние**.

  Значок DeviceLock отображается в области уведомлений, если в настройках сервиса включена опция Всегда отображать значок в системной области.

- Сервис DeviceLock отправляет журналы аудита и теневого копирования на сервер DeviceLock Enterprise Server.
- Сетевой интерфейс меняет состояние:
  - Сетевой кабель подключен или отключен.
  - Модем подключается или отключается.
  - Подключение по виртуальной частной сети (VPN) устанавливается или разрывается.
  - Беспроводное WiFi соединение устанавливается или разрывается.
  - Назначенный DHCP-сервером IP-адрес используется или освобождается.
  - Сетевая карта включена, отключена, добавлена или удалена.
- Меняются настройки сервиса DeviceLock.

Управление политиками безопасности для автономного режима (устройства)

В данном разделе приводятся базовые процедуры управления политиками безопасности для автономного режима, которые аналогичны политикам безопасности для автономного режима. Подробнее о разрешениях, аудите, правилах теневого копирования, тревожных оповещениях, белых списках, настройках безопасности и контентно-зависимых правилах для устройств см. в следующих разделах:

Разрешения (обычный профиль)

Аудит, теневое копирование и алерты (обычный профиль)

Белый список USB-устройств (обычный профиль)

Белый список носителей (обычный профиль)

Настройки безопасности (обычный профиль)

Правила для устройств в главе Контентно-зависимые правила (обычный профиль)

Управление политиками для устройств для автономного режима предполагает:

- Управление разрешениями
- Управление правилами аудита, теневого копирования и оповещений
- Управление белым списком USB-устройств
- Управление белым списком носителей
- Управление контентно-зависимыми правилами
- Управление настройками безопасности

Управлять политиками безопасности для автономного режима можно с помощью консоли DeviceLock Management Console, Service Settings Editor или DeviceLock Group Policy Manager.

Управление разрешениями

Подробное описание функциональности разрешений см. в разделе Разрешения (обычный профиль).

Разрешения для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - Настройки разрешений для данного протокола не заданы.
- **Задано** - Разным учетным записям назначены разные разрешения для устройств данного типа.
- **Полный доступ** - У всех учетных записей есть полный доступ к устройствам данного типа.

  Это состояние отображается, например, когда разрешения заданы только для учетной записи "Все" (Everyone) таким образом, что у нее есть полный доступ к устройствам.
- **Нет доступа** - Нет учетных записей, имеющих доступ к устройствам данного типа.

  Это состояние отображается, например, когда учетной записи "Все" (Everyone) явно запрещен любой доступ к устройствам данного типа или разрешения не заданы ни для каких учетных записей. Обратите внимание, что запрет для учетной записи "Все" (Everyone) отменяет все разрешения для других учетных записей.
- **Использовать обычный** - Наследование разрешений для автономного режима заблокировано и принудительно применяются разрешения для оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение разрешений для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование разрешений для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении разрешений для оперативного режима см. в разделе Удаление всех разрешений, заданных для автономного режима.

Управление разрешениями для автономного режима предполагает:

- Задание и редактирование разрешений
- Сброс разрешений
- Удаление всех разрешений, заданных для автономного режима

Задание и редактирование разрешений

Чтобы задать или редактировать разрешения

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства** выберите **Разрешения**.

   Если в дереве консоли выбрать "Разрешения", на панели сведений отобразятся типы устройств, для которых можно установить разрешения. На панели сведений в столбце "Офлайн" также отображается текущее состояние разрешений на каждый тип устройств для автономного режима.

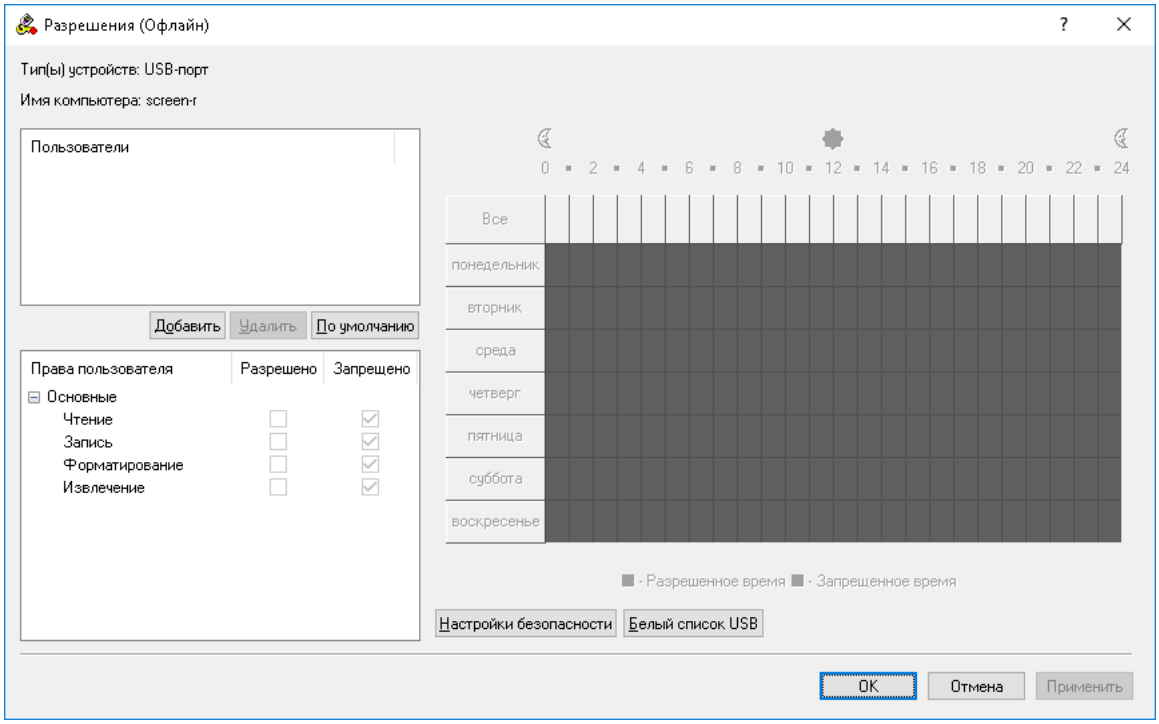
4. На панели сведений выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши тип устройств, для которого требуется задать или редактировать разрешения, а затем выберите команду **Установить офлайновые разрешения**.

     - или -

   - Выберите тип устройств, для которого требуется установить или редактировать разрешения, а затем щелкните значок **Установить офлайновые разрешения** на панели инструментов.

Появится диалоговое окно “Разрешения (Офлайн)”.



5. В диалоговом окне **Разрешения (Офлайн)** выполните следующее:

Чтобы установить разрешения по умолчанию

- В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **По умолчанию**.

  Таким образом разрешения по умолчанию устанавливаются для учетных записей “Администраторы”, “Все” и “Система”. Для получения информации о том, какие разрешения предоставляются этим учетным записям по умолчанию, см. раздел Разрешения (обычный профиль).

Чтобы настроить разрешения для нового пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”

b) В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой верхней части диалогового окна “Разрешения (Офлайн)”.

c) В левой верхней части диалогового окна **Разрешения (Офлайн)** в области **Пользователи** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

d) На левой нижней панели диалогового окна **Разрешения (Офлайн)** в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

   В правой части диалогового окна “Разрешения (Офлайн)” можно указать дни недели и время, когда будет предоставлен доступ к устройствам. Используйте левую кнопку мыши, чтобы выбрать дни недели и время, когда выбранному пользователю или группе будет предоставлен доступ к устройствам. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда доступ будет запрещен.

Чтобы изменить разрешения для имеющегося пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу.

b) На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

Чтобы удалить имеющегося пользователя или группу и разрешения

- В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или клавишу DELETE.

6. Нажмите кнопку **OK** или **Применить**.

Сброс разрешений

Можно вернуть ранее заданные разрешения в исходное “неопределенное” состояние. Если разрешения для автономного режима находятся в исходном “неопределенном” состоянии, к клиентским компьютерам, работающим автономно, применяются разрешения для оперативного режима.

Чтобы вернуть разрешения в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства** выберите **Разрешения**.

   Если в дереве консоли выбрать “Разрешения”, на панели сведений отобразятся типы устройств, для которых можно установить разрешения. На панели сведений в столбце “Офлайн” также отображается текущее состояние разрешений на каждый тип устройств для автономного режима.

4. На панели сведений щелкните правой кнопкой мыши тип устройства, для которого требуется вернуть разрешения в исходное “неопределенное” состояние, а затем выберите команду **Сбросить офлайновые настройки**.

   Можно вернуть разрешения в исходное “неопределенное” состояние для нескольких типов устройств одновременно. Чтобы это сделать, выполните следующее:

   a) На панели сведений выберите несколько типов устройств, удерживая клавишу SHIFT или CTRL и щелкая типы устройств.

   b) Щелкните правой кнопкой мыши выбранные протоколы, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние разрешений для автономного режима изменится на “Не задано”.

Удаление всех разрешений, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование разрешений для автономного режима от объектов более высокого уровня и принудительно применять разрешения для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение разрешений для оперативного режима, необходимо удалить разрешения для автономного режима.

Чтобы удалить разрешения

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства** выберите **Разрешения**.

   Если в дереве консоли выбрать "Разрешения", на панели сведений отобразятся типы устройств, для которых можно установить разрешения. На панели сведений в столбце "Офлайн" также отображается текущее состояние разрешений на каждый тип устройств для автономного режима.

4. На панели сведений щелкните правой кнопкой мыши тип устройства, для которого требуется удалить разрешения для автономного режима, а затем выберите команду **Удалить офлайновые настройки**.

   Можно удалить разрешения для автономного режима для нескольких типов устройств одновременно. Чтобы это сделать, выполните следующее:

   a) На панели сведений выберите несколько типов устройств, удерживая клавишу SHIFT или CTRL и щелкая типы устройств.

   b) Щелкните правой кнопкой мыши выбранные протоколы, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние разрешений для автономного режима изменится на "Использовать обычный."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление правилами аудита, теневого копирования и оповещений

Описание функции аудита и теневого копирования для устройств см. в разделе Аудит, теневое копирование и алерты (обычный профиль). Описание функции тревожных оповещений см. в разделе Алерты. О включении оповещений для оперативного режима см. Аудит, теневое копирование и алерты (обычный профиль). О включении оповещений для автономного режима см. Включение тревожных оповещений далее в этом разделе.

Аудит, правила теневого копирования и алерты для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - Аудит, правила теневого копирования и тревожные оповещения в автономном режиме для данного типа устройств не заданы.
- **Задано** - Для данного типа устройств в автономном режиме заданы аудит, правила теневого копирования и/или тревожные оповещения.
- **Нет аудита** - Настройки для данного типа устройств не разрешают аудит, теневое копирование и тревожные оповещения ни для каких учетных записей.
- **Использовать обычный** - Наследование правил автономного режима заблокировано и принудительно применяются правила оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение правил оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование правил для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении правил оперативного режима см. в разделе Удаление всех правил аудита и теневого копирования, заданных для автономного режима.

Управление правилами аудита, теневого копирования и оповещений для автономного режима предполагает:

- Задание и редактирование правил аудита и теневого копирования
- Включение тревожных оповещений
- Сброс правил аудита и теневого копирования
- Удаление всех правил аудита и теневого копирования, заданных для автономного режима

Задание и редактирование правил аудита и теневого копирования

Чтобы задать и редактировать правила аудита и теневого копирования

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства** выберите **Аудит, Теневое копирование и Алерты**.

   Если в дереве консоли выбрать "Аудит, Теневое копирование и Алерты", на панели сведений отобразятся типы устройств, для которых можно задавать правила аудита и теневого копирования. На панели сведений в столбце "Офлайн" также отображается текущее состояние правил для автономного режима для каждого типа устройств.

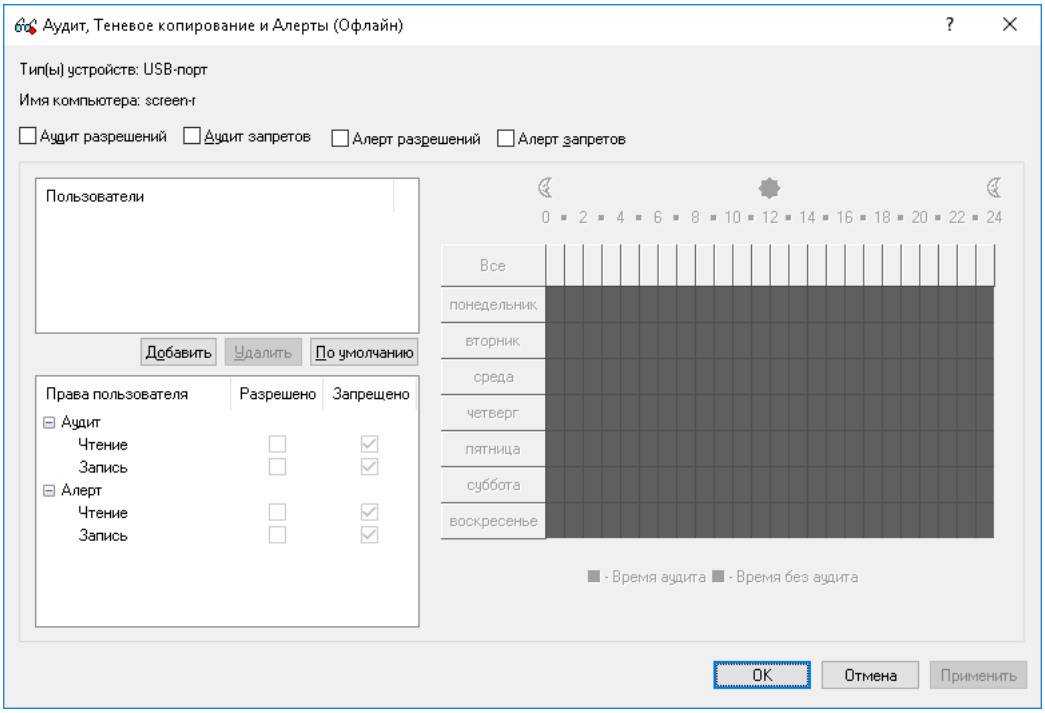
4. На панели сведений выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши тип устройств, для которого требуется задать или редактировать правила, а затем выберите команду **Установить офлайновый аудит, теневое копирование и алерты**.

     - или -

   - Выберите тип устройств, для которого требуется задать или редактировать правила, а затем щелкните значок **Установить офлайновый аудит, теневое копирование и алерты** на панели инструментов.

Появится диалоговое окно “Аудит, Теневое копирование и Алерты (Офлайн)”.



5. В диалоговом окне **Аудит, Теневое копирование и Алерты (Офлайн)** выполните следующее:

   Чтобы задать правила аудита и теневого копирования по умолчанию

   a) В левой верхней части диалогового окна укажите, какие события записываются в журнал аудита. Установите флажок **Аудит разрешений**, чтобы регистрировать успешные попытки доступа к устройству. Установите флажок **Аудит запретов**, чтобы регистрировать неудачные попытки доступа к устройству.

   b) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **По умолчанию**.

      По умолчанию правила аудита и теневого копирования задаются для членов группы “Пользователи” (Users) и учетной записи “Все” (Everyone). Для получения информации о том, какие права аудита и теневого копирования предоставляются этим учетным записям по умолчанию, см. раздел Аудит, теневое копирование и алерты (обычный профиль).

Чтобы настроить правила аудита и теневого копирования для нового пользователя или группы

a) В левой верхней части диалогового окна укажите, какие события записываются в журнал аудита. Установите флажок **Аудит разрешений**, чтобы регистрировать успешные попытки доступа к устройству. Установите флажок **удит запретов**, чтобы регистрировать неудачные попытки доступа к устройству.

b) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**.

c) В появившемся диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.

Добавленные пользователи и группы отображаются в области "Пользователи" в левой верхней части диалогового окна "Аудит, Теневое копирование и Алерты (Офлайн)".

d) В левой верхней части диалогового окна **Аудит, Теневое копирование и Алерты (Офлайн)** в области **Пользователи** выберите пользователя или группу.

Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

e) На левой нижней панели диалогового окна **Аудит, Теневое копирование и Алерты (Офлайн)** в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

Права аудита и теневого копирования определяют, какие действия пользователя записываются в журнал аудита и журнал теневого копирования.

В правой части диалогового окна "Аудит, Теневое копирование и Алерты (Офлайн)" можно указать дни недели и время (например, с 7 часов утра до 5 часов вечера с понедельника по пятницу), когда действия выбранных пользователей будут записываться в журнал аудита или теневого копирования. Используйте левую кнопку мыши, чтобы выбрать дни недели и время, когда действия выбранных пользователей будут записываться в журнал. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда действия пользователей не будут записываться в журнал.

Чтобы изменить правила аудита и теневого копирования для имеющегося пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу.

b) На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

Чтобы удалить имеющегося пользователя или группу и правило

- В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или клавишу DELETE.

  При удалении пользователя или группы, все правила для него также удаляются.

6. Нажмите кнопку **OK** или **Применить**.

Включение тревожных оповещений

Оповещения для автономного режима о событиях, связанных с попытками доступа, можно включить в диалоговом окне **Аудит, Теневое копирование и Алерты (Офлайн)**. Оповещения для автономного режима включаются так же, как задаются правила аудита для автономного режима (см. Задание и редактирование правил аудита и теневого копирования), в следующем порядке:

- Укажите, для каких событий необходимо рассылать оповещения. Оповещения можно настроить для попыток доступа к устройству (как удачных, так и неудачных). Установите флажок **Алерт разрешений**, чтобы включить оповещения об успешных попытках доступа к устройству. Установите флажок **Алерт запретов**, чтобы включить оповещения о неудачных попытках доступа к устройству.
- Укажите пользователей и/или группы, на действия которых будут рассылаться оповещения. Для этого в левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.
- Укажите, на какие действия пользователей нужно рассылать оповещения, а на какие нет. В левой верхней части диалогового окна в области **Пользователи** выберите добавленного пользователя или группу. На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить право на алерт. Эти права определяют, на какие действия пользователя с устройствами следует рассылать оповещения. Права на алерт аналогичны правам на аудит. Единственное различие состоит в том, что при наступлении событий, удовлетворяющих определенным критериям, DeviceLock отправляет оповещение вместо записи в журнале аудита. Подробную информацию о правах на аудит устройств см. в разделе Аудит, теневое копирование и алерты (обычный профиль).
- Укажите дни и часы (например, с 7 утра до 5 вечера с понедельника по пятницу), в которые оповещения о действиях пользователя с устройствами будут или не будут рассылаться. Для этого на правой панели диалогового окна выберите дни и часы левой кнопкой мыши. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда на действия пользователей не будут рассылаться оповещения.

Сброс правил аудита и теневого копирования

Можно вернуть ранее заданные правила аудита и теневого копирования в исходное "неопределенное" состояние. Если правила для автономного режима находятся в исходном "неопределенном" состоянии, к клиентским компьютерам, работающим автономно, применяются правила для оперативного режима.

Чтобы вернуть правила в исходное "неопределенное" состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства** выберите **Аудит, Теневое копирование и Алерты**.

   Если в дереве консоли выбрать "Аудит, Теневое копирование и Алерты", на панели сведений отобразятся типы устройств, для которых можно задавать правила аудита, теневого копирования и оповещений. На панели сведений в столбце "Офлайн" также отображается текущее состояние правил для автономного режима для каждого типа устройств.

4. На панели сведений щелкните правой кнопкой мыши тип устройства, для которого требуется вернуть правила в исходное "неопределенное" состояние, а затем выберите команду **Сбросить офлайновые настройки**.

   Можно вернуть правила аудита и теневого копирования в исходное "неопределенное" состояние для нескольких типов устройств одновременно. Чтобы это сделать, выполните следующее:

   a) На панели сведений выберите несколько типов устройств, удерживая клавишу SHIFT или CTRL и щелкая типы устройств.

   b) Щелкните правой кнопкой мыши выбранные протоколы, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние правил аудита и теневого копирования для автономного режима изменится на "Не задано".

Удаление всех правил аудита и теневого копирования, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование правил аудита и теневого копирования для автономного режима от объектов более высокого уровня и принудительно применять правила для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение правил аудита и теневого копирования для оперативного режима, необходимо удалить правила аудита и теневого копирования для автономного режима.

Чтобы удалить правила аудита и теневого копирования

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства** выберите **Аудит, Теневое копирование и Алерты**.

   Если в дереве консоли выбрать "Аудит, Теневое копирование и Алерты", на панели сведений отобразятся типы устройств, для которых можно задавать правила аудита, теневого копирования и оповещений. На панели сведений в столбце "Офлайн" также отображается текущее состояние правил для автономного режима для каждого типа устройств.
4. На панели сведений щелкните правой кнопкой мыши тип устройства, для которого требуется удалить правила аудита и теневого копирования для автономного режима, а затем выберите команду **Удалить офлайновые настройки**.

   Можно удалить правила аудита и теневого копирования для автономного режима для нескольких типов устройств одновременно. Чтобы это сделать, выполните следующее:
   a) На панели сведений выберите несколько типов устройств, удерживая клавишу SHIFT или CTRL и щелкая типы устройств.
   b) Щелкните правой кнопкой мыши выбранные протоколы, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние правил аудита и теневого копирования для автономного режима изменится на "Использовать обычный".

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление белым списком USB-устройств

Подробное описание функциональности белого списка USB-устройств см. в разделе Белый список USB-устройств (обычный профиль).

Белый список USB-устройств для автономного режима может иметь одно из следующих состояний:

- **Не задано** - Белый список не задан. Содержит следующее сообщение: “Офлайновый белый список USB не задан.” Это состояние отображается по умолчанию.
- **Задано** - Белый список задан.
- **Использовать обычный** - Наследование белого списка для автономного режима блокируется и принудительно применяется белый список для оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение белого списка для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование белого списка для автономного режима от объектов более высокого уровня.

  Дополнительную информацию о принудительном применении белого списка для оперативного режима см. в разделе Удаление белого списка USB-устройств, заданного для автономного режима.

Управление белым списком USB-устройств для автономного режима предполагает:

- Задание и редактирование белого списка USB-устройств
- Экспорт и импорт белого списка USB-устройств
- Сброс белого списка USB-устройств
- Удаление белого списка USB-устройств, заданного для автономного режима

Задание и редактирование белого списка USB-устройств

Чтобы задать и редактировать белый список USB-устройств

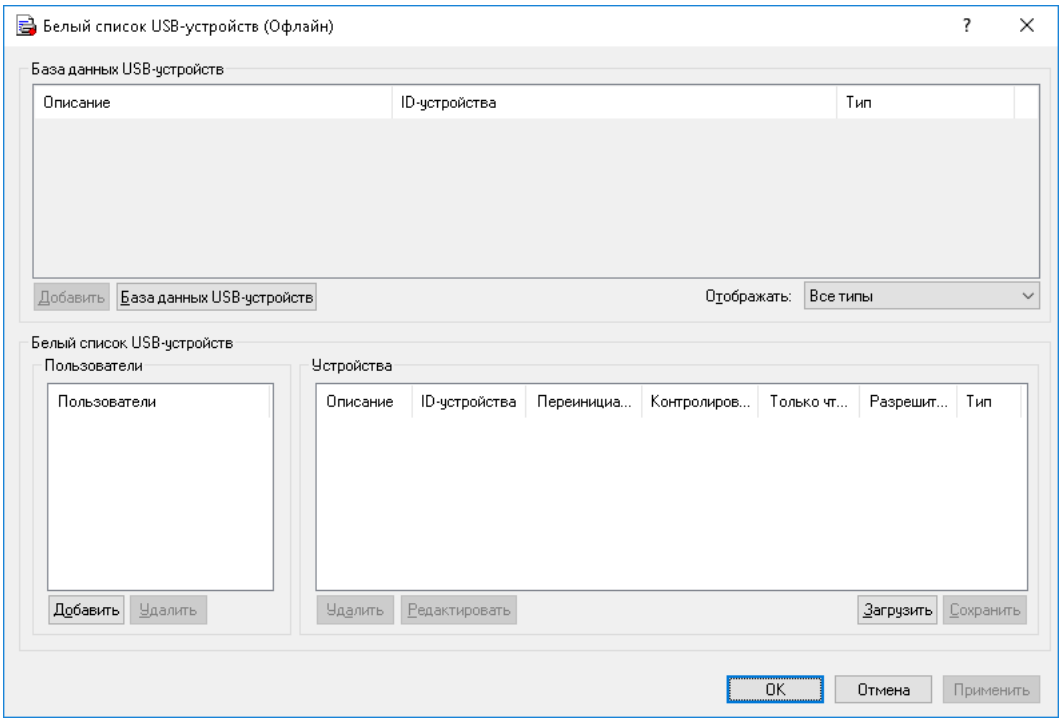
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Белый список USB-устройств**, а затем выберите команду **Управление офлайновыми настройками**.

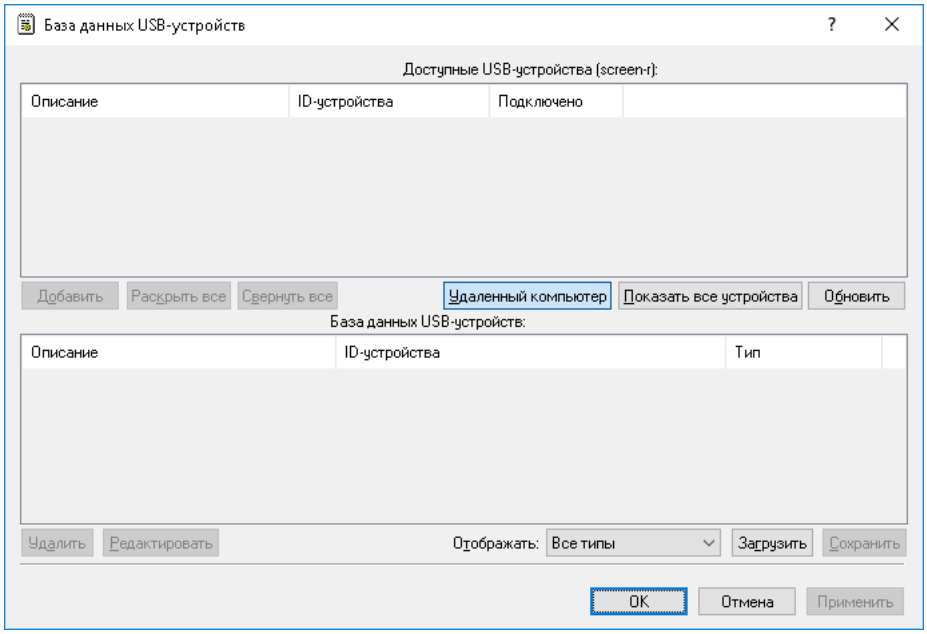
     - или -
   - Выберите **Белый список USB-устройств**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

   Появится диалоговое окно "Белый список USB-устройств (Офлайн)".



4. В верхней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **База данных USB-устройств**, нажмите кнопку **База данных USB-устройств**.

Появится диалоговое окно “База данных USB-устройств”.



В верхней части диалогового окна “База данных USB-устройств” в области “Доступные USB-устройства” отображаются подключенные в настоящий момент устройства.

Чтобы просмотреть все устройства, которые когда-либо были подключены к компьютеру, нажмите кнопку **Показать все устройства**. Чтобы получить список устройств с удаленного компьютера, нажмите кнопку **Удаленный компьютер**.

Кнопка “Удаленный компьютер” недоступна, когда консоль подключена к локальному компьютеру.

5. В верхней части диалогового окна **База данных USB-устройств** в области **Доступные USB-устройства** выберите устройство, которое требуется добавить в белый список, а затем нажмите кнопку **Добавить**.

   Добавленное устройство отображается в области “База данных USB-устройств” в нижней части диалогового окна “База данных USB-устройств”.

Примечание: Добавить устройство в белый список USB-устройств можно только после того, как устройство внесено в базу данных USB-устройств.

Для белого списка USB-устройств для обоих режимов (оперативного и автономного) используется одна и та же база данных USB-устройств.

Чтобы удалить устройство из базы данных устройств, в нижней части диалогового окна **База данных USB-устройств** в области **База данных USB-устройств** выполните одно из следующих действий:

- Выберите устройство, а затем нажмите кнопку **Удалить**.

  - или -

- Щелкните правой кнопкой мыши устройство, а затем выберите команду **Удалить**.

После удаления устройств из базы данных устройств они не удаляются автоматически из белого списка.

Для редактирования описания устройства в нижней части диалогового окна **База данных USB-устройств** в области **База данных USB-устройств** выберите устройство, а затем нажмите кнопку **Редактировать**.

При изменении описания устройства в базе данных устройств наблюдается следующее поведение: устройство, уже добавленное в белый список, сохранит свое прежнее описание.

6. Нажмите кнопку **OK** или **Применить**.

   Устройства, добавленные в базу данных USB-устройств, отображаются в области "База данных USB-устройств" в верхней части диалогового окна "Белый список USB-устройств (Офлайн)".

7. В левой нижней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно Выбор: "Пользователи" или "Группы".

8. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать белый список USB-устройств, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области "Пользователи" в левой нижней части диалогового окна "Белый список USB-устройств (Офлайн)".

   Чтобы удалить пользователя или группу, в левой нижней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **Пользователи** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или клавишу DELETE.

9. В левой нижней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **Пользователи** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

10. В верхней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **База данных USB-устройств** выберите устройство, которое требуется добавить в белый список для выбранного пользователя или группы, а затем нажмите кнопку **Добавить**.

    Чтобы выбрать одновременно несколько устройств, используйте клавиши SHIFT или CTRL.

    Добавленные в белый список устройства отображаются в области "Устройства" в правой нижней части диалогового окна.

Чтобы удалить устройство из белого списка для выбранного пользователя или группы, в правой нижней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **Устройства** выполните следующее:

- Выберите устройство, а затем нажмите кнопку **Удалить**.

  - или -

- Щелкните правой кнопкой мыши устройство, а затем выберите команду **Удалить**.

  - или -

- Выберите устройство, а затем нажмите клавишу DELETE.

Чтобы редактировать описание устройства, в правой нижней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **Устройства** выполните следующее:

- Выберите устройство, а затем нажмите кнопку **Редактировать**.

  - или -

- Щелкните правой кнопкой мыши устройство, а затем выберите команду **Редактировать**.

11. Нажмите кнопку **OK** или **Применить**.

Экспорт и импорт белого списка USB-устройств

Можно экспортировать белый список USB-устройств для автономного режима в файл с расширением .whl, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт белого списка также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать белый список USB-устройств

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Белый список USB-устройств**, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Выберите **Белый список USB-устройств**, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Раскройте **Белый список USB-устройств**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Раскройте **Белый список USB-устройств**, выберите любого пользователя или группу, указанную в белом списке. На панели сведений щелкните правой кнопкой мыши устройство, внесенное в белый список, а затем выберите команду **Сохранить**.

     - или -
   - Щелкните правой кнопкой мыши **Белый список USB-устройств**, а затем выберите команду **Управление офлайновыми настройками**. В правой нижней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **Устройства** нажмите кнопку **Сохранить**.
4. В появившемся диалоговом окне выберите папку для сохранения файла, задайте имя файла, и нажмите кнопку **Сохранить**.

   При экспорте белый список USB-устройств сохраняется в файле с расширением whl.

Чтобы импортировать белый список USB-устройств

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.

3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Белый список USB-устройств**, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -
   - Выберите **Белый список USB-устройств**, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -
   - Раскройте **Белый список USB-устройств**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -
   - Раскройте **Белый список USB-устройств**, выберите любого пользователя или группу, указанную в белом списке. На панели сведений щелкните правой кнопкой мыши носитель, внесенный в белый список, а затем выберите команду **Загрузить**.

     - или -
   - Щелкните правой кнопкой мыши **Белый список USB-устройств**, а затем выберите команду **Управление офлайновыми настройками**. В правой нижней части диалогового окна **Белый список USB-устройств (Офлайн)** в области **Устройства** нажмите кнопку **Загрузить**.
4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

Сброс белого списка USB-устройств

Можно вернуть ранее заданный белый список протоколов в исходное “неопределенное” состояние. Если белый список для автономного режима находится в исходном “неопределенном” состоянии, к клиентским компьютерам, работающим автономно, применяется белый список для оперативного режима.

Чтобы вернуть белый список USB-устройств в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.

3. В узле **Устройства** щелкните правой кнопкой мыши **Белый список USB-устройств**, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние белого списка для автономного режима изменится на "Не задано."

   Теперь, если в дереве консоли выбрать узел **Белый список USB-устройств**, на панели сведений выводится следующее сообщение: "Офлайновый белый список USB не задан."

Удаление белого списка USB-устройств, заданного для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование белого списка для автономного режима от объектов более высокого уровня и принудительно применять белый список для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение белого списка USB-устройств для оперативного режима, необходимо удалить белый список USB-устройств для автономного режима.

Чтобы удалить белый список USB-устройств

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, щелкните правой кнопкой мыши **Белый список USB-устройств**, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние белого списка для автономного режима изменится на "Использовать обычный".

   Теперь, если в дереве консоли выбрать узел **Белый список USB-устройств**, на панели сведений выводится следующее сообщение: "Офлайновый белый список USB использует конфигурацию обычного белого списка".

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление белым списком носителей

Подробное описание функциональности белого списка носителей см. в разделе Белый список носителей (обычный профиль).

Белый список носителей для автономного режима может иметь одно из следующих состояний:

- **Не задано** - Блый список не задан. Содержит следующее сообщение: “Офлайновый белый список носителей не задан.” Это состояние отображается по умолчанию.
- **Задано** - Белый список задан.
- **Использовать обычный** - Наследование белого списка для автономного режима блокируется и принудительно применяется белый список для оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение белого списка для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование белого списка для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении белого списка для оперативного режима см. в разделе Удаление белого списка носителей, заданного для автономного режима.

Управление белым списком носителей для автономного режима предполагает:

- Задание и редактирование белого списка носителей
- Экспорт и импорт белого списка носителей
- Сброс белого списка носителей
- Удаление белого списка носителей, заданного для автономного режима

Задание и редактирование белого списка носителей

Чтобы задать и редактировать белый список носителей

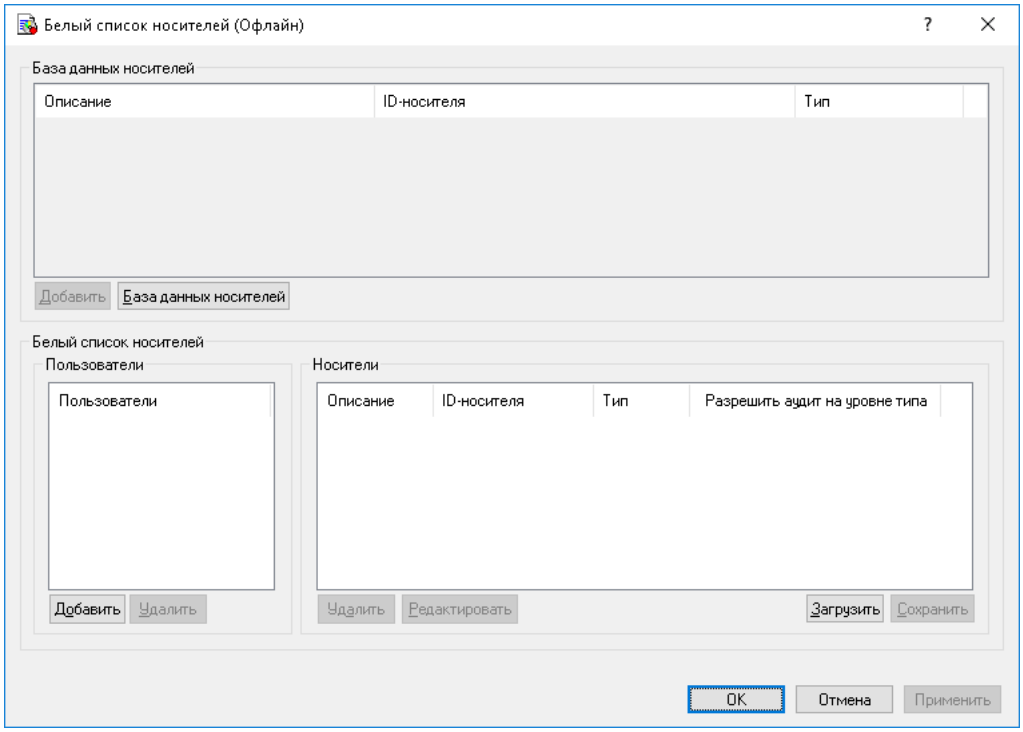
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Белый список носителей**, а затем выберите команду **Управление офлайновыми настройками**.

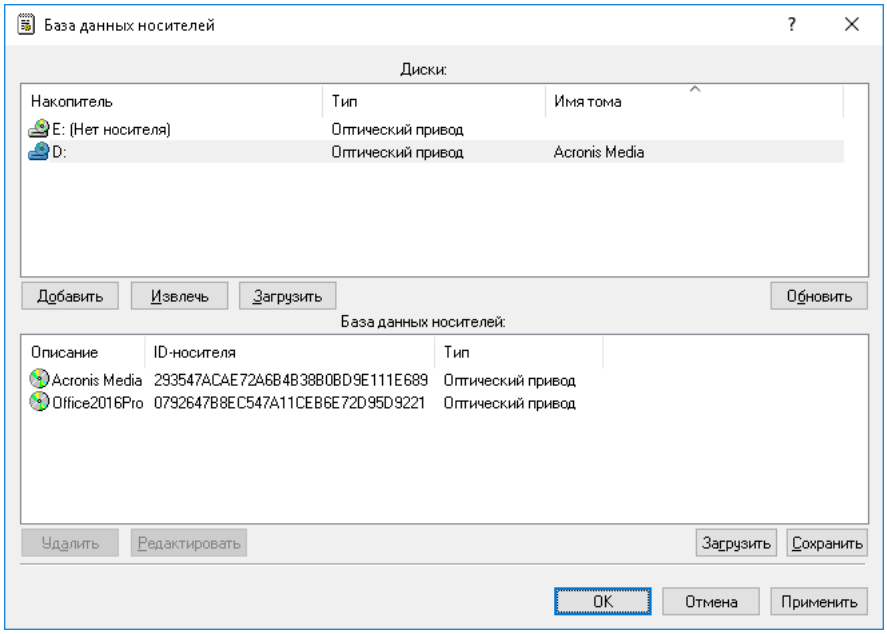
     - или -
   - Выберите **Белый список носителей**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

   Появится диалоговое окно "Белый список носителей (Офлайн)".



4. В верхней части диалогового окна **Белый список носителей (Офлайн)** в области **База данных носителей**, нажмите кнопку **База данных носителей**.

Появится диалоговое окно "База данных носителей".



В верхней части диалогового окна "База данных носителей" в области "Диски" отображаются все CD/DVD/BD-ROM дисководы, доступные на локальном компьютере.

Список дисководов и носителей обновляется автоматически по мере их появления. Чтобы вручную обновить этот список, нажмите кнопку "Обновить".

5. В верхней части диалогового окна **База данных носителей** в области **Диски** выберите дисковод, содержащий носитель, который требуется добавить в белый список, а затем нажмите кнопку **Добавить**.

   Выбранные носители добавляются в базу данных носителей и отображаются в нижней части диалогового окна "База данных носителей".

   > **Примечание:** Добавить носитель в белый список носителей можно только после того, как носитель внесен в базу данных носителей.
   >
   > Для белого списка носителей для обоих режимов (оперативного и автономного) используется одна и та же база данных носителей.

   Чтобы удалить носитель из базы данных носителей, в нижней части диалогового окна **База данных носителей** выполните одно из следующих действий:

   - Выберите носитель, а затем нажмите кнопку **Удалить**.

     - или -

   - Щелкните правой кнопкой мыши носитель, а затем выберите команду **Удалить**.

   Для редактирования описания носителя в нижней части диалогового окна **База данных носителей** выберите носитель, а затем нажмите кнопку **Редактировать**.

6. Нажмите кнопку **OK** или **Применить**.

   Носители, добавленные в базу данных, отображаются в области "База данных носителей" в верхней части диалогового окна "Белый список носителей (Офлайн)".

7. В левой нижней части диалогового окна **Белый список носителей (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

8. В появившемся диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать белый список носителей, и нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области "Пользователи" в левой нижней части диалогового окна "Белый список носителей (Офлайн)".

   Чтобы удалить пользователя или группу, в левой нижней части диалогового окна **Белый список носителей (Офлайн)** в области **Пользователи** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или клавишу DELETE.

9. В левой нижней части диалогового окна **Белый список носителей (Офлайн)** в области **Пользователи** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

10. В верхней части диалогового окна **Белый список носителей (Офлайн)** в области **База данных носителей** выберите носитель, который требуется добавить в белый список для выбранного пользователя или группы, а затем нажмите кнопку **Добавить**.

    Чтобы выбрать одновременно несколько носителей, используйте клавиши SHIFT или CTRL.

    Добавленные в белый список носители отображаются в области "Носители" в правой нижней части диалогового окна.

    Чтобы удалить носитель из белого списка для выбранного пользователя или группы, в правой нижней части диалогового окна **Белый список носителей (Офлайн)** в области **Носители** выполните следующее:

    - Выберите носитель, а затем нажмите кнопку **Удалить**.

      - или -

    - Щелкните правой кнопкой мыши носитель, а затем выберите команду **Удалить**.

    Чтобы редактировать описание носителя, в правой нижней части диалогового окна **Белый список носителей (Офлайн)** в области **Носители** выполните следующее:

    - Выберите носитель, а затем нажмите кнопку **Редактировать**.

      - или -

    - Щелкните правой кнопкой мыши носитель, а затем выберите команду **Редактировать**.

11. Нажмите кнопку **OK** или **Применить**.

Экспорт и импорт белого списка носителей

Можно экспортировать белый список носителей для автономного режима в файл с расширением .mwl, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт правил также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать белый список носителей

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Белый список носителей**, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Выберите **Белый список носителей**, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Раскройте **Белый список носителей**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Раскройте **Белый список носителей**, выберите любого пользователя или группу, указанную в белом списке. На панели сведений щелкните правой кнопкой мыши носитель, внесенный в белый список, а затем выберите команду **Сохранить**.

     - или -
   - Щелкните правой кнопкой мыши **Белый список носителей**, а затем выберите команду **Управление офлайновыми настройками**. В правой нижней части диалогового окна **Белый список носителей (Офлайн)** в области **Носители** нажмите кнопку **Сохранить**.
4. В появившемся диалоговом окне выберите папку для сохранения файла, задайте имя файла, и нажмите кнопку **Сохранить**.

   При экспорте белый список носителей сохраняется в файле с расширением .mwl.

Чтобы импортировать белый список носителей

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства**, выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Белый список носителей**, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Выберите **Белый список носителей**, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -

   - Раскройте **Белый список носителей**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Раскройте **Белый список носителей**, выберите любого пользователя или группу, указанную в белом списке. На панели сведений щелкните правой кнопкой мыши носитель, внесенный в белый список, а затем выберите команду **Загрузить**.

     - или -

   - Щелкните правой кнопкой мыши **Белый список носителей**, а затем выберите команду **Управление офлайновыми настройками**. В правой нижней части диалогового окна **Белый список носителей (Офлайн)** в области **Носители** нажмите кнопку **Загрузить**.

4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

Сброс белого списка носителей

Можно вернуть ранее заданный белый список протоколов в исходное “неопределенное” состояние. Если белый список для автономного режима находится в исходном “неопределенном” состоянии, к клиентским компьютерам, работающим автономно, применяется белый список для оперативного режима.

Чтобы вернуть белый список носителей в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера,** а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства** щелкните правой кнопкой мыши **Белый список носителей**, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние белого списка для автономного режима изменится на “Не задано”.

   Теперь, если в дереве консоли выбрать узел **Белый список носителей**, на панели сведений выводится следующее сообщение: “Офлайновый белый список носителей не задан.”

Удаление белого списка носителей, заданного для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование белого списка для автономного режима от объектов более высокого уровня и принудительно применять белый список для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение белого списка носителей для оперативного режима, необходимо удалить белый список носителей для автономного режима.

Чтобы удалить белый список носителей

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, щелкните правой кнопкой мыши **Белый список носителей**, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние белого списка для автономного режима изменится на "Использовать обычный".

   Теперь, если в дереве консоли выбрать узел **Белый список носителей**, на панели сведений выводится следующее сообщение: "Офлайновый белый список носителей использует конфигурацию обычного белого списка."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление контентно-зависимыми правилами

Подробное описание контентно-зависимых правил для устройств см. в разделе Правила для устройств главы Контентно-зависимые правила (обычный профиль).

Контентно-зависимые правила для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - Контентно-зависимые правила не заданы. Содержит следующее сообщение: "Офлайновые контентно-зависимые правила не заданы." Это состояние отображается по умолчанию.
- **Задано** - Контентно-зависимые правила заданы.
- **Использовать обычный** - Наследование контентно-зависимых правил для автономного режима блокируется и принудительно применяются контентно-зависимые правила для оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение контентно-зависимых правил для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование контентно-зависимых правил для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении контентно-зависимых правил для оперативного режима см. в разделе Удаление всех контентно-зависимых правил, заданных для автономного режима.

Управление контентно-зависимыми правилами для автономного режима предполагает:

- Создание контентно-зависимых правил
- Редактирование контентно-зависимых правил
- Копирование контентно-зависимых правил
- Экспорт и импорт контентно-зависимых правил
- Удаление отдельных контентно-зависимых правил
- Сброс контентно-зависимых правил
- Удаление всех контентно-зависимых правил, заданных для автономного режима

Создание контентно-зависимых правил

Контентно-зависимые правила создаются на основе встроенных или пользовательских контентных групп. Для получения подробной информации об этих контентных группах см. раздел Настройка контентных групп.

Вы можете включить тревожные оповещения о том, что сработало контентно-зависимое правило. Такие оповещения включаются при настройке контентно-зависимого правила.

DeviceLock рассылает тревожные оповещения с учетом соответствующих настроек. В этих настройках задается адресат и способ отправки оповещений. Перед включением оповещений для контентно-зависимых правил задайте параметры оповещений в настройках сервиса DeviceLock (см. раздел Алерты).

Чтобы создать контентно-зависимое правило

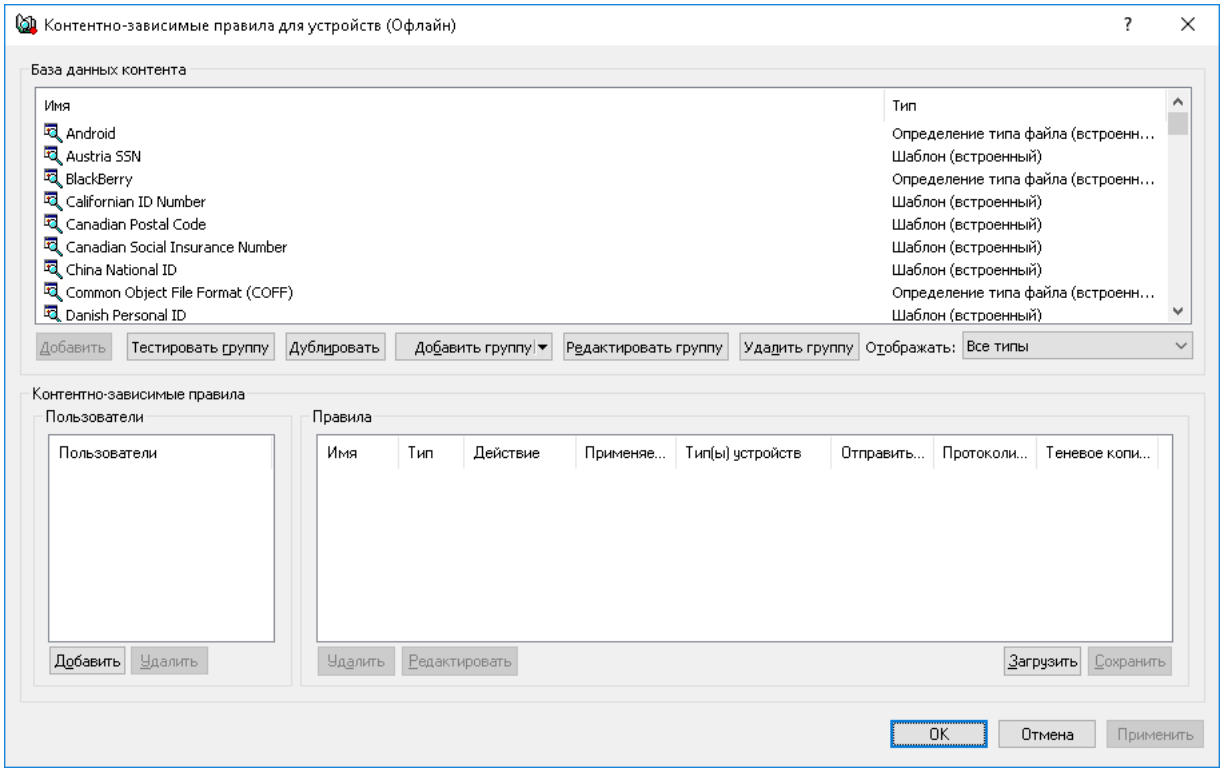
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

Появится диалоговое окно “Контентно-зависимые правила для устройств (Офлайн)”.



4. В левой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.
5. В появившемся диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать правило, а затем нажмите кнопку **OK**.

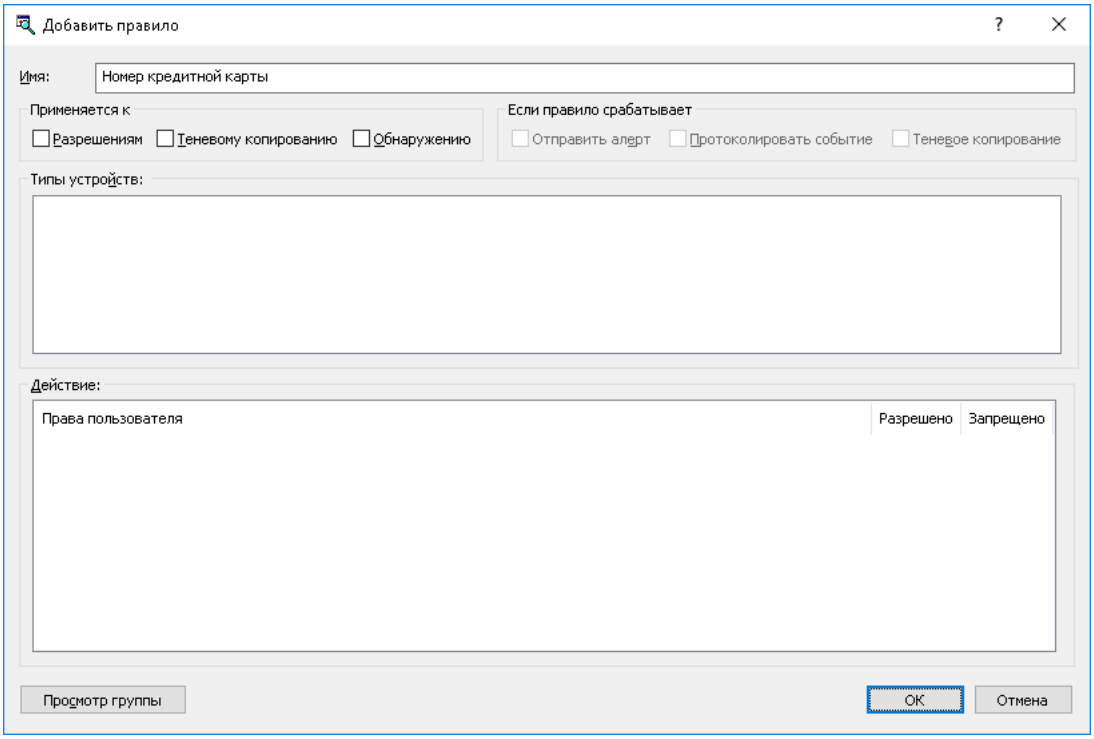
   Добавленные пользователи и группы отображаются в области “Пользователи” в левой нижней части диалогового окна “Контентно-зависимые правила для устройств (Офлайн)”.

   Чтобы удалить пользователя или группу, в области **Пользователи** в левой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или нажмите клавишу DELETE.
6. В левой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Пользователи** выберите пользователя или группу, для которой требуется задать правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.
7. В верхней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **База данных контента** выберите необходимую контентную группу, а затем нажмите кнопку **Добавить**, или дважды щелкните необходимую контентную группу.

   Примечание: Для каждого создаваемого контентно-зависимого правила можно указать только одну контентную группу.

Появится диалоговое окно “Добавить правило”.



8. В диалоговом окне **Добавить правило** в поле **Имя** введите имя контентно-зависимого правила.

   Имя правила по умолчанию совпадает с именем его контентной группы. При необходимости имя правила может быть изменено.

   Для просмотра контентной группы данного правила нажмите кнопку **Просмотр группы** в левом нижнем углу диалогового окна. Консоль отображает свойства группы в отдельном диалоговом окне, позволяя просматривать свойства, но не изменять их.

9. В области **Применяется к** укажите тип операций, к которым должно применяться это правило. Возможные варианты:
   - **Разрешениям** - Указывает, что правило применяется к операциям контроля доступа.
   - **Теневому копированию** - Указывает, что правило применяется к операциям теневого копирования.
   - **Обнаружению** - Указывает, что правило будет обнаруживать указанное содержимое передаваемых данных, при этом будут протоколироваться события обнаружения и отправляться тревожные уведомления, если установлены соответствующие флаги.
   - **Разрешениям**, **Теневому копированию** - Указывает, что правило применяется и к операциям контроля доступа, и к операциям теневого копирования.
   - **Разрешениям, Обнаружению** - Указывает, что правило будет применяться как для операция контроля, так и для операций обнаружения.
   - **Теневому копированию, Обнаружению** - Указывает, что правило будет применяться как для операций избирательного теневого копирования, так и для операций обнаружения.
   - **Разрешениям, Теневому копированию, Обнаружению** - Указывает, что правило будет применяться как для операций контроля и избирательного теневого копирования, так и для операций обнаружения.

   Примечание: Для успешного создания/сохранения правила, применяемого исключительно к операциям обнаружения или же к к операциям обнаружения в совокупности с другими операциями, необходимо выбрать по крайней мере одну из следующих опций для правила: **Протоколировать событие**, **Отправить алерт** или **Теневое копирование** (см. шаг 10 данной процедуры). В противном случае, такое правило не сохраняется, и показывается следующее сообщение: "Необходимо выбрать флаг Протоколировать событие, Отправить алерт или Теневое копирование."

10. В области **Если правило срабатывает** укажите следующие дополнительные операции, которые будут выполняться при срабатывании оповещения:
    - **Отправить алерт** - Оповещение рассылается при каждом срабатывании правила.
    - **Протоколировать событие** - Событие регистрируется в журнале аудита при каждом срабатывании правила.
    - **Теневое копирование** - Теневая копия данных создается при каждом срабатывании правила.

    При включении или отключении алертов, аудита и/или теневого копирования в контентно-зависимом правиле настройка правила имеет приоритет над соответствующей настройкой для типа устройств.

    Пример: Если аудит включен для некоторого типа устройств и отключен в правиле для этого типа устройств, срабатывание такого правила не вызовет события аудита. Если же аудит в правиле включен, то срабатывание правила вызовет событие аудита, даже если аудит отключен на уровне типа устройств.

    Правило может наследовать настройку алертов, аудита и/или теневого копирования, заданную на уровне типа устройств. Эта опция выбрана по умолчанию и представлена неопределенным состоянием флажков (не установленных и не очищенных). Состояние каждого флажка можно изменить независимо от других.

    Пример: Если правило наследует настройку аудита, заданную для типа устройств, то срабатывание такого правила вызовет событие аудита только если аудит включен для типа устройств, контролируемых этим правилом.

11. В области **Типы устройств** выберите типы устройств, к которым должно применяться это правило.

    Контентно-зависимые правила могут применяться к следующим типам устройств: Буфер обмена, Гибкий диск, iPhone-устройства, MTP, Оптический привод, Palm, Принтер, Съемные устройства, TC-устройства и Windows Mobile"

12. В области **Действие** укажите, какие действия с файлами пользователю разрешены или запрещены, какие действия пользователя будут записываться в журнале теневого копирования, а также какие действия пользователя будут трактоваться как события обнаружения содержимого.

    Если правило применяется одновременно к операциям контроля доступа и операциям теневого копирования, то опция "Чтение" будет недоступна. О правах, которые могут быть заданы в контентно-зависимых правилах, см. разделы Управление доступом к контенту, Теневое копирование контента и Обнаружение контента для устройств.

13. Нажмите кнопку **OK**.

    Созданное правило отображается в области "Правила" в правой нижней части диалогового окна "Контентно-зависимые правила для устройств (Офлайн)".

14. Нажмите кнопку **OK** или **Применить**, чтобы применить правило.

Пользователи и группы, для которых заданы контентно-зависимые правила, отображаются в дереве консоли в узле **Контентно-зависимые правила**. Если в дереве консоли выбрать пользователя или группу, для которой задано правило, на панели сведений отобразится информация о заданном правиле (подробнее см. в разделе Список контентно-зависимых правил для устройств).

Можно задавать контентно-зависимые правила для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Для получения информации о том, как задать контентно-зависимые правила для оперативного режима, см. раздел Управление контентно-зависимыми правилами в главе Контентно-зависимые правила (обычный профиль).

Редактирование контентно-зависимых правил

Можно редактировать свойства заданных контентно-зависимых правил, такие как **Имя**, **Применяется к**, **Если правило срабатывает, Типы устройств, Действие**.

Чтобы редактировать контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства**, щелкните правой кнопкой мыши **Контентно-зависимые правила**, выберите команду **Управление офлайновыми настройками**, а затем выполните следующее:

   a) В левой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Пользователи** выберите пользователя или группу, для которой задано правило, которое требуется редактировать.

   Если выбрать пользователей или группы, в области "Правила" в правой нижней части диалогового окна отображаются контентно-зависимые правила, которые применяются к этим пользователям или группам.

   b) В правой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Правила** выберите правило, которое требуется редактировать, а затем нажмите кнопку **Редактировать**.

   - или -

   Щелкните правой кнопкой мыши правило, а затем выберите команду **Редактировать**.

   - или -

   Дважды щелкните правило.

   - или -

   В узле **Устройства** раскройте **Контентно-зависимые правила**, а затем выполните следующее:

   a) В узле **Контентно-зависимые правила** выберите пользователя или группу, для которой требуется редактировать правило.

   Если выбрать пользователей или группы, на панели сведений консоли отображаются контентно-зависимые правила, которые применяются к этим пользователям или группам.

   b) На панели сведений щелкните правой кнопкой мыши правило, которое требуется редактировать, а затем выберите команду **Редактировать**.

   Появится диалоговое окно "Редактирование правила".

4. В диалоговом окне **Редактирование правила** внесите необходимые изменения.
5. Нажмите кнопку **OK**, чтобы применить изменения.

Копирование контентно-зависимых правил

Можно выполнять операции вырезать-вставить, копировать-вставить, а также операции перетаскивания, чтобы повторно использовать существующие контентно-зависимые правила для автономного режима.

Чтобы скопировать контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

   Появится диалоговое окно "Контентно-зависимые правила для устройств (Офлайн)".
4. В левой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Пользователи** выберите пользователя или группу, к которой применяется правило, которое требуется скопировать.

   Если выбрать пользователей или группы, в области "Правила" в правой нижней части диалогового окна отображаются контентно-зависимые правила, которые применяются к этим пользователям или группам.
5. В правой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Правила** щелкните правой кнопкой мыши правило, которое требуется скопировать, а затем выберите команду **Копировать** или **Вырезать**.

   Вырезанное или скопированное правило автоматически копируется в буфер обмена.

   Также можно использовать сочетания клавиш CTRL+C, CTRL+X и CTRL+V, чтобы скопировать, вырезать и вставить правило. При нажатии CTRL+X правило будет вырезано только после того, как вы его вставите.

   Для выполнения операции перетаскивания, выделите правило и перетащите его к пользователю или группе, к которой требуется применить скопированное правило.

6. В левой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

7. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых должно применяться скопированное правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой нижней части диалогового окна “Контентно-зависимые правила для устройств (Офлайн)”.

8. В левой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Пользователи** выберите пользователей или группы, для которых требуется задать скопированное правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

9. В правой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** щелкните правой кнопкой мыши в области **Правила**, а затем выберите команду **Вставить**.

   Скопированное правило отображается в области “Правила” в правой нижней части диалогового окна “Контентно-зависимые правила для устройств (Офлайн)”.

10. Нажмите кнопку **OK** или **Применить**, чтобы применить скопированное правило.

Экспорт и импорт контентно-зависимых правил

Можно экспортировать все заданные контентно-зависимые правила для автономного режима в файл с расширением .cwl, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт правил также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать контентно-зависимые правила

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши любого пользователя или группу, для которой задано правило, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой правило, а затем выберите команду **Сохранить**.

     - или -
   - Раскройте **Контентно-зависимые правилas**, выберите любого пользователя или группу, для которой задано правило, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**. В правой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Правила** нажмите кнопку **Сохранить**.
4. В появившемся диалоговом окне выберите папку, в которую требуется сохранить файл, задайте имя файла, и нажмите кнопку **Сохранить**.

   При экспорте правила сохраняются в файле с расширением .cwl.

Чтобы импортировать контентно-зависимые правила

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства**, выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -

   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши любого пользователя или группу, для которой задано правило, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, а затем выберите команду **Загрузить**.

     - или -

   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**. В правой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Правила** нажмите кнопку **Загрузить**.

4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

   За один раз можно импортировать только один файл .cwl.

Удаление отдельных контентно-зависимых правил

Можно удалять отдельные контентно-зависимые правила для автономного режима, если они больше не нужны.

Чтобы удалить отдельное контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства**, выполните одно из следующих действий:

   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши пользователя или группу, для которой задано правило, а затем выберите команду **Удалить пользователя**.

     Если удалить пользователя или группу, все правила, заданные для этого пользователя или группы, автоматически удалятся.

     - или -

   - Раскройте **Контентно-зависимые правила**, затем выберите пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, заданное для этого пользователя или группы, а затем выберите команду **Удалить**.

     - или -

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**. В левой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Пользователи** выберите пользователя или группу, для которой задано правило. В правой нижней части диалогового окна **Контентно-зависимые правила для устройств (Офлайн)** в области **Правила** выберите правило и затем нажмите кнопку **Удалить** или щелкните правой кнопкой мыши правило и затем выберите команду **Удалить**.

     Чтобы выбрать одновременно несколько правил, используйте клавиши SHIFT или CTRL.

Сброс контентно-зависимых правил

Можно вернуть ранее заданные контентно-зависимые правила в исходное “неопределенное” состояние. Если правила для автономного режима находятся в исходном “неопределенном” состоянии, к клиентским компьютерам, работающим автономно, применяются правила для оперативного режима.

Чтобы вернуть контентно-зависимые правила в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства** щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние контентно-зависимых правил для автономного режима изменится на “Не задано”.

   Если в дереве консоли выбрать **Контентно-зависимые правила**, на панели сведений выводится следующее сообщение: “Офлайновые контентно-зависимые правила не заданы.”

Удаление всех контентно-зависимых правил, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование контентно-зависимых правил для автономного режима от объектов более высокого уровня и принудительно применять контентно-зависимые правила для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение контентно-зависимых правил для оперативного режима, необходимо удалить контентно-зависимые правила для автономного режима.

Чтобы удалить все заданные контентно-зависимые правила

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства**, щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние контентно-зависимых правил для автономного режима изменится на "Использовать обычный."

   Если в дереве консоли выбрать **Контентно-зависимые правила**, на панели сведений выводится следующее сообщение: "Офлайновые контентно-зависимые правила используют конфигурацию обычных правил."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление настройками безопасности

Подробное описание функциональности настроек безопасности см. в разделе Настройки безопасности (обычный профиль).

Настройки безопасности для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - Показывает, что настройки безопасности не заданы. Это состояние отображается по умолчанию.
- **Включено** - Показывает, что настройки безопасности заданы: включен аудит и контроль доступа для указанных классов устройств.
- **Отключено** - Показывает, что настройки безопасности заданы: отключен аудит и контроль доступа для указанных классов устройств.
- **Использовать обычный** - Показывает, что наследование настроек безопасности для автономного режима блокируется и принудительно применяются настройки безопасности для оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение настроек безопасности для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование настроек безопасности для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении настроек безопасности для оперативного режима см. в разделе Удаление всех настроек безопасности, заданных для автономного режима.

Управление настройками безопасности для автономного режима предполагает:

- Задание и редактирование настроек безопасности
- Сброс настроек безопасности
- Удаление всех настроек безопасности, заданных для автономного режима

Задание и редактирование настроек безопасности

Настройки безопасности для автономного режима можно задавать и изменять все сразу или по отдельности.

Чтобы задать и редактировать настройки безопасности по отдельности

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства** выберите **Настройки безопасности**.

   Если в дереве консоли выбрать "Настройки безопасности", на панели сведений отобразятся настройки безопасности.
4. На панели сведений щелкните правой кнопкой мыши нужную настройку безопасности, а затем выберите команду **Включить офлайн**.

   Состояние настройки безопасности для автономного режима изменится с "Не задано" на "Включено".

   Включенную настройку безопасности можно отключить. Для этого щелкните правой кнопкой мыши нужную настройку, а затем выберите команду **Выключить офлайн**.

   Состояние настройки безопасности для автономного режима изменится с "Включено" на "Отключено."

Чтобы задать и редактировать настройки безопасности совместно

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.

3. В узле **Устройства**, выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Настройки безопасности**, а затем выберите команду **Управление офлайновыми настройками**.

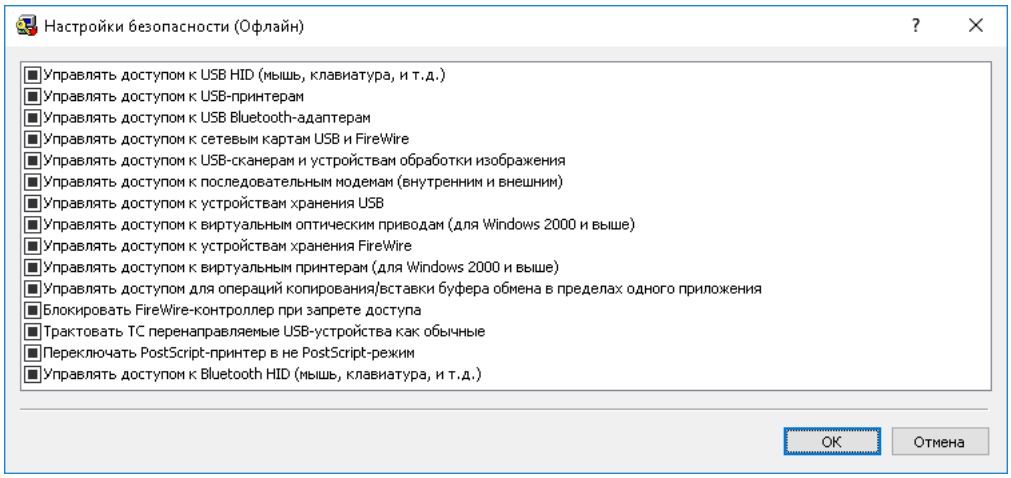
     - или -
   - Выберите **Настройки безопасности**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

     - или -
   - Выберите **Настройки безопасности**. На панели сведений щелкните правой кнопкой мыши любую настройку безопасности, а затем выберите команду **Управление офлайновыми настройками**.

     - или -
   - Выберите **Настройки безопасности**. На панели сведений выберите любую настройку безопасности, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

     Если в дереве консоли выбрать "Настройки безопасности", на панели сведений отобразятся настройки безопасности.

   Появится диалоговое окно "Настройки безопасности (Офлайн)".



4. В диалоговом окне **Настройки безопасности (Офлайн)** установите флажки для настроек безопасности, которые требуется задать.

   Включенные настройки безопасности можно отключить. Для этого необходимо снять флажки для настроек, которые требуется отключить.

   Примечание: Все флажки в диалоговом окне **Настройки безопасности (Офлайн)** могут иметь одно из трех состояний: установленные, снятые или в неопределенном состоянии, что соответствует состояниям **Включено**, **Отключено** и **Не задано** настроек безопасности.

5. Нажмите кнопку **OK**.

Сброс настроек безопасности

Можно вернуть ранее заданные настройки безопасности в исходное “неопределенное” состояние. Если настройки для автономного режима находятся в исходном “неопределенном” состоянии, к клиентским компьютерам, работающим автономно, применяются настройки для оперативного режима.

Чтобы вернуть настройки безопасности в исходное “неопределенное” состояние по отдельности

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства** выберите **Настройки безопасности**.

   Если в дереве консоли выбрать “Настройки безопасности”, на панели сведений отобразятся настройки безопасности.
4. На панели сведений щелкните правой кнопкой мыши нужную настройку безопасности, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние настройки безопасности для автономного режима изменится на “Не задано”.

Чтобы вернуть сразу все настройки безопасности в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Устройства**.

3. В узле **Устройства**, выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Настройки безопасности**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -

   - Выберите **Настройки безопасности**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

     - или -

   - Выберите **Настройки безопасности**. На панели сведений щелкните правой кнопкой мыши любую настройку безопасности, а затем выберите команду **Управление офлайновыми настройками**.

     - или -

   - Выберите **Настройки безопасности**. На панели сведений выберите любую настройку безопасности, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

     Если в дереве консоли выбрать “Настройки безопасности”, на панели сведений отобразятся настройки безопасности.

4. В появившемся диалоговом окне **Настройки безопасности (Офлайн)** задайте неопределенное состояние для настроек безопасности.

   Примечание: Все флажки в этом диалоговом окне могут иметь одно из трех состояний: установленные, снятые или в неопределенном состоянии, что соответствует состояниям **Включено**, **Отключено** и **Не задано** настроек безопасности.

Удаление всех настроек безопасности, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование настроек безопасности для автономного режима от объектов более высокого уровня и принудительно применять настройки безопасности для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение настроек безопасности для оперативного режима, необходимо удалить настройки безопасности для автономного режима. Настройки безопасности для автономного режима удаляются по отдельности.

Чтобы удалить настройки безопасности

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Устройства**.
3. В узле **Устройства** выберите **Настройки безопасности**.

   Если в дереве консоли выбрать "Настройки безопасности", на панели сведений отобразятся настройки безопасности.
4. На панели сведений щелкните правой кнопкой мыши настройку безопасности, которую необходимо удалить, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние настройки безопасности для автономного режима изменится на "Использовать обычный."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление политиками безопасности для автономного режима (протоколы)

Управление политиками для протоколов для автономного режима предполагает:

- Управление разрешениями
- Управление правилами аудита, теневого копирования и оповещений
- Управление белым списком протоколов
- Управление базовым IP-файрволом
- Управление контентно-зависимыми правилами
- Управление настройками безопасности

Управлять политиками безопасности для автономного режима можно с помощью консоли DeviceLock Management Console, Service Settings Editor или DeviceLock Group Policy Manager.

Управление разрешениями

Подробное описание функциональности разрешений для протоколов см. в разделе Разрешения на доступ к протоколам для оперативного режима.

Разрешения для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - Настройки разрешений для данного протокола не заданы.
- **Задано** - Разным учетным записям назначены разные разрешения для данного протокола.
- **Полный доступ** - У всех учетных записей есть полный доступ к данному протоколу.

  Это состояние отображается, например, когда разрешения заданы только для учетной записи “Все” (Everyone) таким образом, что у нее есть полный доступ к протоколу.
- **Нет доступа** - Нет учетных записей, имеющих доступ к данному протоколу.

  Это состояние отображается, например, когда учетной записи “Все” (Everyone) явно запрещен любой доступ к данному протоколу или разрешения не заданы ни для каких учетных записей. Обратите внимание, что запрет для учетной записи “Все” (Everyone) отменяет любые разрешения для других учетных записей.
- **Использовать обычный** - Наследование разрешений для автономного режима заблокировано и принудительно применяются разрешения для оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение разрешений для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование разрешений для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении разрешений для оперативного режима см. в разделе Удаление всех разрешений, заданных для автономного режима.

Управление разрешениями для автономного режима предполагает:

- Задание и редактирование разрешений
- Сброс разрешений
- Удаление всех разрешений, заданных для автономного режима

Задание и редактирование разрешений

Чтобы задать или редактировать разрешения

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выберите **Разрешения**.

   Если в дереве консоли выбрать "Разрешения", на панели сведений отобразятся протоколы, для которых можно установить разрешения. На панели сведений в столбце "Офлайн" также отображается текущее состояние разрешений на каждый протокол для автономного режима.

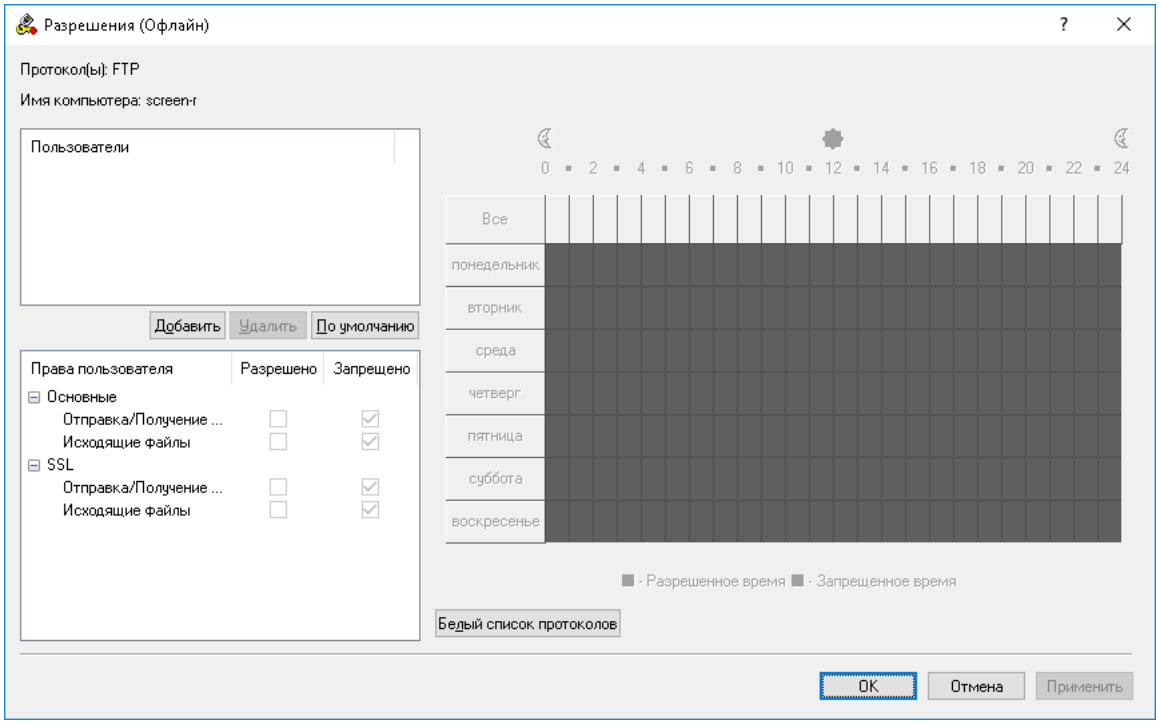
4. На панели сведений выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши протокол, для которого требуется задать или редактировать разрешения, а затем выберите команду **Установить офлайновые разрешения**.

     - или -

   - Выберите протокол, для которого требуется установить или редактировать разрешения, а затем щелкните значок **Установить офлайновые разрешения** на панели инструментов.

Появится диалоговое окно “Разрешения (Офлайн)”.



5. В диалоговом окне **Разрешения (Офлайн)** выполните следующее:

Чтобы установить разрешения по умолчанию

- В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **По умолчанию**.

  Таким образом разрешения по умолчанию устанавливаются для учетных записей “Администраторы” и “Все”. Для получения информации о том, какие разрешения предоставляются этим учетным записям по умолчанию, см. раздел см. в разделе Разрешения на доступ к протоколам.

Чтобы настроить разрешения для нового пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**.

b) В появившемся диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.

Добавленные пользователи и группы отображаются в области "Пользователи" в левой верхней части диалогового окна "Разрешения (Офлайн)".

c) В левой верхней части диалогового окна **Разрешения (Офлайн)** в области **Пользователи** выберите пользователя или группу.

Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

d) На левой нижней панели диалогового окна **Разрешения (Офлайн)** в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

В правой части диалогового окна "Разрешения (Офлайн)" можно указать дни недели и время, когда будет предоставлен доступ к выбранным протоколам. Используйте левую кнопку мыши, чтобы выбрать дни недели и время, когда выбранному пользователю или группе будет предоставлен доступ к выбранным протоколам. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда доступ будет запрещен.

Чтобы изменить разрешения для имеющегося пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу.

b) На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

Чтобы удалить имеющегося пользователя или группу и разрешения

- В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или клавишу DELETE.

  Если удалить пользователя или группу, разрешения, установленные для этого пользователя или группы, будут автоматически удалены.

Чтобы задать, просмотреть или изменить правила белого списка для данного протокола

- Нажмите кнопку **Белый список протоколов**. Подробнее о белом списке протоколов для автономного режима см. в разделе Управление белым списком протоколов данной главы.

Чтобы задать, просмотреть или изменить настройки безопасности для протокола MAPI

- Нажмите кнопку **Настройки безопасности**. Подробнее о настройках безопасности протоколов для автономного режима см. в разделе Управление настройками безопасности данной главы.

  Примечание: Кнопка **Настройки безопасности** появляется в диалоговом окне **Разрешения (Офлайн)** только при управлении разрешениями для протокола MAPI. Для других протоколов эта кнопка отсутствует.

6. Нажмите кнопку **OK** или **Применить**.

Сброс разрешений

Можно вернуть ранее заданные разрешения в исходное “неопределенное” состояние. Если разрешения для автономного режима находятся в исходном “неопределенном” состоянии, к клиентским компьютерам, работающим автономно, применяются разрешения для оперативного режима.

Чтобы вернуть разрешения в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выберите **Разрешения**.

   Если в дереве консоли выбрать “Разрешения”, на панели сведений отобразятся протоколы, для которых можно установить разрешения. На панели сведений в столбце “Офлайн” также отображается текущее состояние разрешений на каждый протокол для автономного режима.

4. На панели сведений щелкните правой кнопкой мыши протокол, для которого требуется вернуть разрешения в исходное “неопределенное” состояние, а затем выберите команду **Сбросить офлайновые настройки**.

   Можно вернуть разрешения в исходное “неопределенное” состояние для нескольких протоколов одновременно. Чтобы это сделать, выполните следующее:

   a) На панели сведений выберите несколько протоколов, удерживая клавишу SHIFT или CTRL и щелкая протоколы.

   b) Щелкните правой кнопкой мыши выбранные протоколы, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние разрешений для автономного режима изменится на “Не задано”.

Удаление всех разрешений, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование разрешений для автономного режима от объектов более высокого уровня и принудительно применять разрешения для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение разрешений для оперативного режима, необходимо удалить разрешения для автономного режима.

Чтобы удалить разрешения

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выберите **Разрешения**.

   Если в дереве консоли выбрать "Разрешения", на панели сведений отобразятся протоколы, для которых можно установить разрешения. На панели сведений в столбце "Офлайн" также отображается текущее состояние разрешений на каждый протокол для автономного режима.
4. На панели сведений щелкните правой кнопкой мыши протокол, для которого требуется удалить разрешения для автономного режима, а затем выберите команду **Удалить офлайновые настройки**.

   Можно удалить разрешения для автономного режима для нескольких протоколов одновременно. Чтобы это сделать, выполните следующее:
   a) На панели сведений выберите несколько протоколов, удерживая клавишу SHIFT или CTRL и щелкая протоколы.
   b) Щелкните правой кнопкой мыши выбранные протоколы, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние разрешений для автономного режима изменится на "Использовать обычный."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление правилами аудита, теневого копирования и оповещений

Подробное описание функциональности аудита и теневого копирования для протоколов см. в разделе Аудит, теневое копирование и алерты для протоколов для оперативного режима. Подробное описание функциональности тревожных оповещений см. в разделе Алерты. Информацию о включении оповещений для протоколов см. в разделе Аудит, теневое копирование и алерты для протоколов. Для получения информации о включении оповещений для автономного режима см. Включение тревожных оповещений далее в этом разделе.

Аудит, правила теневого копирования и алерты для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - Аудит, правила теневого копирования и тревожные оповещения в автономном режиме для данного протокола не заданы.
- **Задано** - Для данного протокола в автономном режиме заданы аудит, правила теневого копирования и/или тревожные оповещения.
- **Нет аудита** - Настройки автономного режима для данного протокола не разрешают аудит, теневое копирование и тревожные оповещения ни для каких учетных записей.
- **Использовать обычный** - Наследование правил автономного режима заблокировано и принудительно применяются правила оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение правил оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование правил для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении правил оперативного режима см. в разделе Удаление всех правил аудита и теневого копирования, заданных для автономного режима.

Управление правилами аудита, теневого копирования и оповещений для автономного режима предполагает:

- Задание и редактирование правил аудита и теневого копирования
- Включение тревожных оповещений
- Сброс правил аудита и теневого копирования
- Удаление всех правил аудита и теневого копирования, заданных для автономного режима

Задание и редактирование правил аудита и теневого копирования

Чтобы задать и редактировать правила аудита и теневого копирования

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выберите **Аудит, Теневое копирование и Алерты**.

   Если в дереве консоли выбрать "Аудит, Теневое копирование и Алерты" на панели сведений отобразятся протоколы, для которых можно задавать правила аудита, теневого копирования и оповещений. На панели сведений в столбце "Офлайн" также отображается текущее состояние правил для автономного режима для каждого протокола.

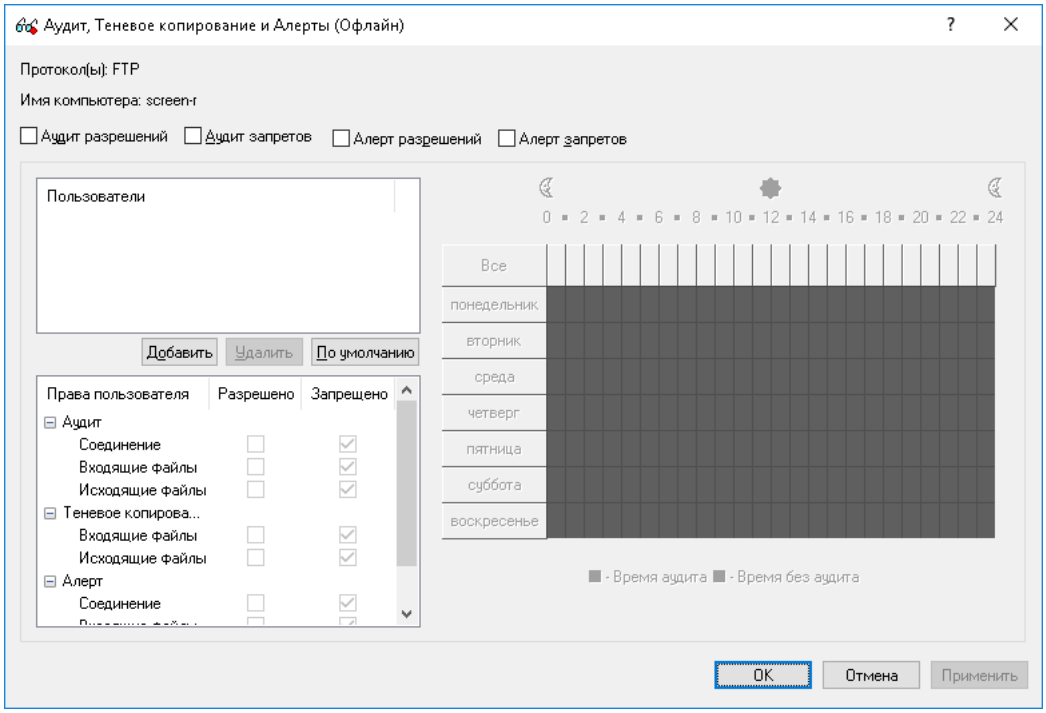
4. На панели сведений выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши протокол, для которого требуется задать или редактировать правила, а затем выберите команду **Установить офлайновый аудит, теневое копирование и алерты**.

     - или -

   - Выберите протокол, для которого требуется задать или редактировать правила, а затем щелкните значок **Установить офлайновый аудит, теневое копирование и алерты** на панели инструментов.

Появится диалоговое окно “Аудит, Теневое копирование и Алерты (Офлайн)”.



5. В диалоговом окне **Аудит, Теневое копирование и Алерты (Офлайн)** выполните следующее:

   Чтобы задать правила аудита и теневого копирования по умолчанию

   a) В левой верхней части диалогового окна укажите, какие события записываются в журнал аудита. Установите флажок **Аудит разрешений**, чтобы регистрировать успешные попытки доступа к протоколу. Установите флажок **Аудит запретов**, чтобы регистрировать неудачные попытки доступа.

   b) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **По умолчанию**.

      По умолчанию правила аудита и теневого копирования задаются для членов групп “Пользователи” (Users) и “Все” (Everyone). Для получения информации о том, какие права аудита и теневого копирования предоставляются этим группам по умолчанию, см. в разделе Аудит, теневое копирование и алерты для протоколов.

Чтобы настроить правила аудита и теневого копирования для нового пользователя или группы

a) В левой верхней части диалогового окна укажите, какие события записываются в журнал аудита. Установите флажок **Аудит разрешений**, чтобы регистрировать успешные попытки доступа к протоколу. Установите флажок **Аудит запретов**, чтобы регистрировать неудачные попытки доступа к протоколу.

b) В левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

c) В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой верхней части диалогового окна “Аудит, Теневое копирование и Алерты (Офлайн)”.

d) В левой верхней части диалогового окна **Аудит, Теневое копирование и Алерты (Офлайн)** в области **Пользователи** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

e) На левой нижней панели диалогового окна **Разрешения (Офлайн)** в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

   Права аудита и теневого копирования определяют, какие действия пользователя записываются в журнал аудита и журнал теневого копирования.

   В правой части диалогового окна “Аудит, Теневое копирование и Алерты (Офлайн)” можно указать дни недели и время (например, с 7 часов утра до 5 часов вечера с понедельника по пятницу), когда действия выбранных пользователей будут записываться в журнал аудита или теневого копирования. Используйте левую кнопку мыши, чтобы выбрать дни недели и время, когда действия выбранных пользователей будут записываться в журнал. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда действия пользователей не будут записываться в журнал.

Чтобы изменить правила аудита и теневого копирования для имеющегося пользователя или группы

a) В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу.

b) На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено**, чтобы включить или отключить соответствующие права.

Чтобы удалить имеющегося пользователя или группу и правило

- В левой верхней части диалогового окна в области **Пользователи** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или клавишу DELETE.

  Если удалить пользователя или группу, правила, заданные для этого пользователя или группы, будут автоматически удалены.

6. Нажмите кнопку **OK** или **Применить**.

Включение тревожных оповещений

Тревожные оповещения для автономного режима о событиях, связанных с попытками доступа, можно включить в диалоговом окне **Аудит, Теневое копирование и Алерты (Офлайн)**. Оповещения для автономного режима включаются так же, как задаются правила аудита для автономного режима (см. Задание и редактирование правил аудита и теневого копирования выше), в следующем порядке:

- Укажите, для каких событий необходимо рассылать оповещения. Оповещения можно настроить для попыток доступа к устройству (как удачных, так и неудачных). Установите флажок **Алерт разрешений**, чтобы включить оповещения об успешных попытках доступа к устройству. Установите флажок **Алерт запроетов**, чтобы включить оповещения о неудачных попытках доступа к устройству.
- Укажите пользователей и/или группы, на действия которых будут рассылаться оповещения. Для этого в левой верхней части диалогового окна в области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.
- Укажите, на какие действия пользователей нужно рассылать оповещения, а на какие нет. В левой верхней части диалогового окна в области **Пользователи** выберите добавленного пользователя или группу. На левой нижней панели диалогового окна в области **Права пользователя** выберите **Разрешено** или **Запрещено** чтобы включить или отключить право на оповещение. Права на оповещения определяют, на какие действия пользователя с устройствами следует рассылать оповещения. Права на оповещение аналогичны правам на аудит. Единственное различие состоит в том, что когда происходят события, удовлетворяющие определенным критериям, DeviceLock отправляет оповещение, а не протоколирует их в журнале аудита. Подробную информацию о правах на аудит устройств см. в разделе Аудит, теневое копирование и алерты для протоколов.
- Укажите дни и часы (например, с 7 утра до 5 вечера с понедельника по пятницу), в которые оповещения о действиях пользователя с устройствами будут или не будут рассылаться. Для этого на правой панели диалогового окна выберите дни и часы левой кнопкой мыши. Используйте правую кнопку мыши, чтобы отметить дни недели и время, когда на действия пользователей не будут рассылаться оповещения.

Сброс правил аудита и теневого копирования

Можно вернуть ранее заданные правила аудита и теневого копирования в исходное "неопределенное" состояние. Если правила для автономного режима находятся в исходном "неопределенном" состоянии, к клиентским компьютерам, работающим автономно, применяются правила для оперативного режима.

Чтобы вернуть правила в исходное "неопределенное" состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел Конфигурация компьютера, а затем раскройте узел DeviceLock.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выберите **Аудит, Теневое копирование и Алерты**.

   Если в дереве консоли выбрать "Аудит, Теневое копирование и Алерты", на панели сведений отобразятся протоколы, для которых можно задавать правила аудита, теневого копирования и оповещений. На панели сведений в столбце "Офлайн" также отображается текущее состояние правил для автономного режима для каждого протокола.

4. На панели сведений щелкните правой кнопкой мыши протокол, для которого требуется вернуть правила в исходное "неопределенное" состояние, а затем выберите команду **Сбросить офлайновые настройки**.

   Можно вернуть правила аудита и теневого копирования в исходное "неопределенное" состояние для нескольких протоколов одновременно. Чтобы это сделать, выполните следующее:

   a) На панели сведений выберите несколько протоколов, удерживая клавишу SHIFT или CTRL и щелкая протоколы.

   b) Щелкните правой кнопкой мыши выбранные протоколы, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние правил аудита и теневого копирования для автономного режима изменится на "Не задано".

Удаление всех правил аудита и теневого копирования, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование правил аудита и теневого копирования для автономного режима от объектов более высокого уровня и принудительно применять правила для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение правил аудита и теневого копирования для оперативного режима, необходимо удалить правила аудита и теневого копирования для автономного режима.

Чтобы удалить правила аудита и теневого копирования

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выберите **Аудит, Теневое копирование и Алерты**.

   Если в дереве консоли выбрать "Аудит, Теневое копирование и Алерты", на панели сведений отобразятся протоколы, для которых можно задавать правила аудита, теневого копирования и оповещений. На панели сведений в столбце "Офлайн" также отображается текущее состояние правил для автономного режима для каждого протокола.
4. На панели сведений щелкните правой кнопкой мыши протокол, для которого требуется удалить правила аудита и теневого копирования для автономного режима, а затем выберите команду **Удалить офлайновые настройки**.

   Можно удалить правила аудита и теневого копирования для автономного режима для нескольких протоколов одновременно. Чтобы это сделать, выполните следующее:
   a) На панели сведений выберите несколько протоколов, удерживая клавишу SHIFT или CTRL и щелкая протоколы.
   b) Щелкните правой кнопкой мыши выбранные протоколы, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние правил аудита и теневого копирования для автономного режима изменится на "Использовать обычный".

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление белым списком протоколов

Подробное описание функциональности белого списка протоколов см. в разделе Белый список протоколов для оперативного режима.

Белый список протоколов для автономного режима может иметь одно из следующих состояний:

- **Не задано** - Показывает, что белый список не задан. Содержит следующее сообщение: “Офлайновый белый список протоколов не задан.” Это состояние отображается по умолчанию.
- **Задано** - Показывает, что белый список задан.
- **Использовать обычный** - Показывает, что наследование белого списка для автономного режима блокируется и принудительно применяется белый список для оперативного режима. Содержит следующее сообщение: “Офлайновый белый список протоколов использует конфигурацию обычного списка протоколов.” Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение белого списка для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование белого списка для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении белого списка для оперативного режима см. в разделе Удаление всех правил белого списка протоколов, заданных для автономного режима.

Управление белым списком протоколов для автономного режима предполагает:

- Задание белого списка протоколов
- Редактирование правил белого списка протоколов
- Копирование правил белого списка протоколов
- Экспорт и импорт белого списка протоколов
- Удаление отдельных правил белого списка протоколов
- Сброс белого списка протоколов
- Удаление всех правил белого списка протоколов, заданных для автономного режима

Задание белого списка протоколов

Чтобы задать белый список протоколов

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

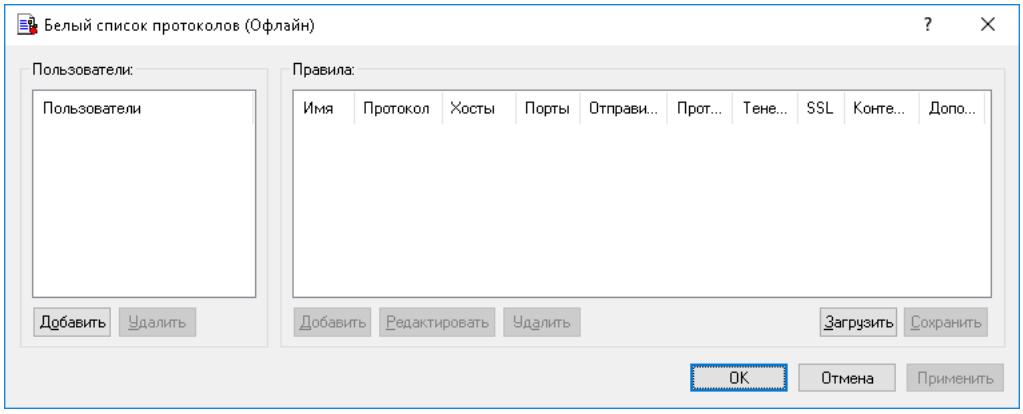
3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -

   - Выберите **Белый список**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

   Появится диалоговое окно "Белый список протоколов (Офлайн)".



4. В левой части диалогового окна **Белый список протоколов (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно "Выбор: "Пользователи" или "Группы"".

5. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать белый список протоколов, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области "Пользователи" в левой части диалогового окна "Белый список протоколов (Офлайн)".

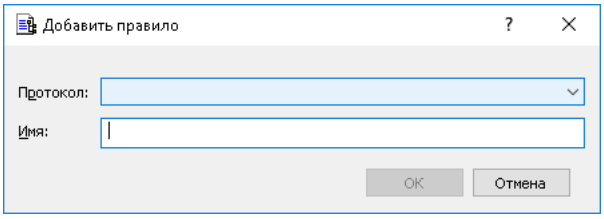
   Чтобы удалить пользователя или группу, в левой части диалогового окна **Белый список протоколов (Офлайн)** в области **Пользователи**, выберите пользователя или группу, а затем нажмите кнопку **Удалить**.

6. В левой части диалогового окна **Белый список протоколов (Офлайн)** в области **Пользователи** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

7. В правой части диалогового окна **Белый список протоколов (Офлайн)** в области **Правила** нажмите кнопку **Добавить**.

   Появится диалоговое окно "Добавить правило".



8. В диалоговом окне **Добавить правило** задайте параметры правила.

   Вначале задайте общие параметры:

   - Чтобы задать протокол, выберите его в списке **Протокол**.
   - Чтобы задать имя правила, ведите его в поле **Имя**.

   Затем задайте параметры, зависящие от выбранного протокола:

   - Чтобы включить проверку контента, установите флажок **Контентный анализ**. Подробнее см. в описании параметра Контентный анализ ранее в этом документе.
   - Чтобы указать дополнительные действия, которые будут выполняться при срабатывании правила, установите соответствующие флажки в области **Если правило срабатывает**. Подробнее см. в описании параметра Если правило срабатывает ранее в этом документе.
   - Чтобы указать узлы, в поле **Хосты** введите имена узлов или IP-адреса через запятую или точку с запятой. Подробнее см. в описании параметра Хосты ранее в этом документе.
   - Чтобы указать порты, в поле **Порты** введите номера портов через запятую или точку с запятой. Подробнее см. в описании параметра Порты ранее в этом документе.
   - Чтобы указать службы файлового обмена и синхронизации, в области **Файловые хранилища** установите соответствующие флажки. Подробнее см. в описании параметра Файловые хранилища ранее в этом документе.
   - Чтобы настроить параметры SSL, в области **SSL** выберите один из следующих вариантов: **Разрешено** (разрешает SSL-соединения), **Запрещено** (запрещает SSL-соединения) или **Обязательно** (требует использования SSL для всех соединений).
   - Чтобы указать идентификаторы локальных отправителей мгновенных сообщений, в поле **ID-локального отправителя** введите идентификаторы пользователей через запятую или точку с запятой. Подробнее см. в описании параметра ID-локального отправителя ранее в этом документе.
   - Чтобы указать получателей мгновенных сообщений, в поле **ID-удаленного получателя** введите идентификаторы пользователей через запятую или точку с запятой. Подробнее см. в описании параметра ID-удаленного получателя ранее в этом документе.
   - Чтобы указать отправителей электронной почты, в поле **E-mail локального отправителя** введите адреса электронной почты, разделенные запятой или точкой с запятой. Подробнее см. в описании параметра E-mail локального отправителя ранее в этом документе.

- Чтобы указать получателей электронной почты, в поле **E-mail удаленного получателя** введите номера портов через запятую или точку с запятой. Подробнее см. в описании параметра E-mail удаленного получателя ранее в этом документе.
- Чтобы указать сайты социальных сетей, установите соответствующие флажки в области **Социальные сети**. Подробнее см. в описании параметра Социальные сети ранее в этом документе.
- Чтобы указать службы веб-почты, установите соответствующие флажки в области **Сервисы Web-почты**. Подробнее см. в описании параметра Сервисы Web-почты ранее в этом документе.
- Чтобы указать провайдеров веб-поиска, установите соответствующие флажки в области **Сервисы Web-поиска**. Подробнее см. в описании параметра Сервисы Web-поиска.
- Чтобы указать провайдеров веб-поиска работы, установите соответствующие флажки в области **Сервисы поиска работы**. Подробнее см. в описании параметра Сервисы поиска работы.

9. Нажмите кнопку **OK**.

   Созданное правило появится в области "Правила" в правой части диалогового окна "Белый список протоколов (Офлайн)".

10. Нажмите кнопку **OK** или **Применить**.

    Пользователи и группы, для которых применяются правила белого списка, отображаются в узле "Белый список" дерева консоли.

Если в дереве консоли выбрать пользователя или группу, к которой применяется правило белого списка, на панели сведений отобразится информация о заданном правиле (подробнее см. в разделе Правила белого списка).

Можно задавать белый список протоколов для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Для получения информации о том, как задать белый список протоколов для оперативного режима, см. раздел Белый список протоколов.

Редактирование правил белого списка протоколов

Можно изменять значения параметров, настроенных для правила белого списка, в любое время.

Чтобы редактировать правило белого списка протоколов

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** щелкните правой кнопкой мыши **Белый список**, выберите команду **Управление офлайновыми настройками**, а затем выполните следующие действия:

   a) В левой части диалогового окна **Белый список протоколов (Офлайн)** в области **Пользователи**, выберите пользователя или группу, для которого требуется изменить правило.

      Если выбрать пользователей или группы, в области "Правила" в правой части диалогового окна отобразятся правила белого списка, которые применяются к этим пользователям или группам.

   b) В правой части диалогового окна **Белый список протоколов (Офлайн)** в области **Правила** выберите правило, которое требуется редактировать, а затем нажмите кнопку **Редактировать**.

      - или -

      Щелкните правой кнопкой мыши правило, а затем выберите команду **Редактировать**.

   - или -

   В узле **Протоколы**, раскройте узел **Белый список**, а затем выполните следующие действия:

   a) В узле **Белый список** выберите пользователя или группу, для которого требуется изменить правило.

      Если выбрать пользователей или группы, на панели сведений отобразятся правила белого списка, которые применяются к этим пользователям или группам.

   b) На панели сведений щелкните правой кнопкой мыши правило, которое требуется редактировать, а затем выберите команду **Редактировать**.

      - или -

      На панели сведений дважды щелкните правило, которое требуется редактировать.

   Появится диалоговое окно "Редактирование правила".

4. В диалоговом окне **Редактирование правила** внесите необходимые изменения.
5. Нажмите кнопку **OK**, чтобы применить изменения.

Копирование правил белого списка протоколов

Можно выполнять операции вырезать-вставить, копировать-вставить, а также операции перетаскивания, чтобы повторно использовать существующие правила белого списка протоколов.

Чтобы скопировать правило белого списка

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -
   - Выберите **Белый список**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

   Появится диалоговое окно "Белый список протоколов (Офлайн)".
4. В левой части диалогового окна **Белый список протоколов (Офлайн)** в области **Пользователи** выберите пользователя или группу, к которой применяется правило, которое требуется скопировать.

   Если выбрать пользователей или группы, в области "Правила" в правой части диалогового окна отобразятся правила белого списка, которые применяются к этим пользователям или группам.
5. В правой части диалогового окна **Белый список протоколов (Офлайн)** в области **Правила** щелкните правой кнопкой мыши правило, которое требуется скопировать, а затем выберите команду **Копировать** или **Вырезать**.

   Вырезанное или скопированное правило автоматически копируется в буфер обмена.

   Также можно использовать сочетания клавиш CTRL+C, CTRL+X и CTRL+V, чтобы скопировать, вырезать и вставить правило. При нажатии CTRL+X правило будет вырезано только после того, как вы его вставите.
6. В левой части диалогового окна **Белый список протоколов (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно "Выбор: "Пользователи" или "Группы"".
7. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых должно применяться скопированное правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области "Пользователи" в левой части диалогового окна "Белый список протоколов (Офлайн)".
8. В левой части диалогового окна **Белый список протоколов (Офлайн)** в области **Пользователи** выберите пользователей или группы, для которых требуется задать скопированное правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.
9. В правой части диалогового окна **Белый список протоколов (Офлайн)** щелкните правой кнопкой мыши в области **Правила**, а затем выберите команду **Вставить**.

   Скопированное правило отображается в области "Правила" в правой части диалогового окна "Белый список протоколов (Офлайн)".
10. Нажмите кнопку **OK** или **Применить**, чтобы применить скопированное правило.

Экспорт и импорт белого списка протоколов

Можно экспортировать все заданные правила белого списка протоколов для автономного режима в файл с расширением .pwl, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт правил также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать белый список протоколов

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Выберите **Белый список**, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Раскройте **Белый список**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Раскройте **Белый список**, выберите любого пользователя или группу, указанную в белом списке. На панели сведений щелкните правой кнопкой правило белого списка, а затем выберите команду **Сохранить**.

     - или -
   - Раскройте **Белый список**, выберите любого пользователя или группу, указанную в белом списке, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление офлайновыми настройками**. В правой части диалогового окна **Белый список протоколов (Офлайн)** в области **Правила** нажмите кнопку **Сохранить**.
4. В появившемся диалоговом окне выберите папку для сохранения файла, задайте имя файла, и нажмите кнопку **Сохранить**.

   При экспорте белый список протоколов сохраняется в файле с расширением .pwl.

Чтобы импортировать белый список протоколов

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Выберите **Белый список**, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -

   - Раскройте **Белый список**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Раскройте **Белый список**, выберите любого пользователя или группу, указанную в белом списке. На панели сведений щелкните правой кнопкой мыши любое правило белого списка, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Раскройте **Белый список**, выберите любого пользователя или группу, указанную в белом списке, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -

   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление офлайновыми настройками**. В правой части диалогового окна **Белый список протоколов (Офлайн)** в области **Правила** нажмите кнопку **Загрузить**.

4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

   Если белый список протоколов для автономного режима уже настроен и вы импортируете новый белый список, появится следующее сообщение: "Вы хотите перезаписать существующие записи (Да - перезаписать, Нет - добавить)?" В окне сообщения нажмите кнопку "Да", чтобы перезаписать существующий белый список. Нажмите кнопку "Нет", чтобы добавить новый список к старому.

Удаление отдельных правил белого списка протоколов

Можно удалять отдельные правила белого списка протоколов для автономного режима, если они больше не нужны.

Чтобы удалить правило белого списка

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Раскройте **Белый список**, щелкните правой кнопкой мыши пользователя или группу, для которой задано правило, а затем выберите команду **Удалить пользователя**.

     Если удалить пользователя или группу, все правила, заданные для этого пользователя или группы, автоматически удалятся.

     - или -
   - Раскройте **Белый список**, затем выберите пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, заданное для этого пользователя или группы, а затем выберите команду **Удалить**.

     - или -
   - Щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление офлайновыми настройками**. В левой части диалогового окна **Белый список протоколов (Офлайн)** в области **Пользователи** выберите пользователя или группу, для которой задано правило. В правой части диалогового окна **Белый список протоколов (Офлайн)** в области **Правила** выберите правило и затем нажмите кнопку **Удалить** или щелкните правой кнопкой мыши правило и затем выберите команду **Удалить**.

Сброс белого списка протоколов

Можно вернуть ранее заданный белый список протоколов в исходное “неопределенное” состояние. Если белый список для автономного режима находится в исходном “неопределенном” состоянии, к клиентским компьютерам, работающим автономно, применяется белый список для оперативного режима.

Чтобы вернуть белый список протоколов в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние белого списка для автономного режима изменится на “Не задано.”

   Если в дереве консоли выбрать **Белый список**, на панели сведений выводится следующее сообщение: “Офлайновый белый список протоколов не задан.”

Удаление всех правил белого списка протоколов, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование белого списка для автономного режима от объектов более высокого уровня и принудительно применять белый список для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение белого списка протоколов для оперативного режима, необходимо удалить белый список протоколов для автономного режима.

Чтобы удалить все заданные правила белого списка протоколов

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние белого списка для автономного режима изменится на "Использовать обычный".

   Если в дереве консоли выбрать узел **Белый список**, на панели сведений выводится следующее сообщение: "Офлайновый белый список протоколов использует конфигурацию обычного списка протоколов."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление базовым IP-файрволом

Подробное описание IP-файрвола см. в разделе Базовый IP-файрвол для оперативного режима.

Правила файрвола для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - IP-файрвол не настроен. Содержит следующее сообщение: "Офлайновый IP-файрвол не задан." Это состояние отображается по умолчанию.
- **Задано** - IP-файрвол настроен.
- **Использовать обычный** - Yаследование правил файрвола для автономного режима блокируется и принудительно применяются обычные правила файрвола. Содержит следующее сообщение: "Офлайновый IP-файрвол использует конфигурацию обычного IP-файрвола." Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение правил файрвола для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование правил файрвола для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении правил файрвола для оперативного режима см. в разделе Удаление всех правил файрвола, заданных для автономного режима.

Управление правилами файрвола для автономного режима предполагает:

- Создание правил файрвола
- Редактирование правил файрвола
- Копирование правил файрвола
- Экспорт и импорт правил файрвола
- Удаление отдельных правил файрвола
- Сброс правил файрвола
- Удаление всех правил файрвола, заданных для автономного режима

Создание правил файрвола

Вы можете включить тревожные оповещения о том, что сработало автономное правило файрвола. Такие оповещения включаются сразу после настройки автономного правила файрвола.

DeviceLock рассылает тревожные оповещения с учетом соответствующих настроек. В этих настройках задается адресат и способ отправки оповещений. Перед тем, как включить оповещения для определенных событий, задайте параметры оповещений в настройках сервиса DeviceLock (см. раздел Алерты).

Чтобы создать правило файрвола для автономного режима

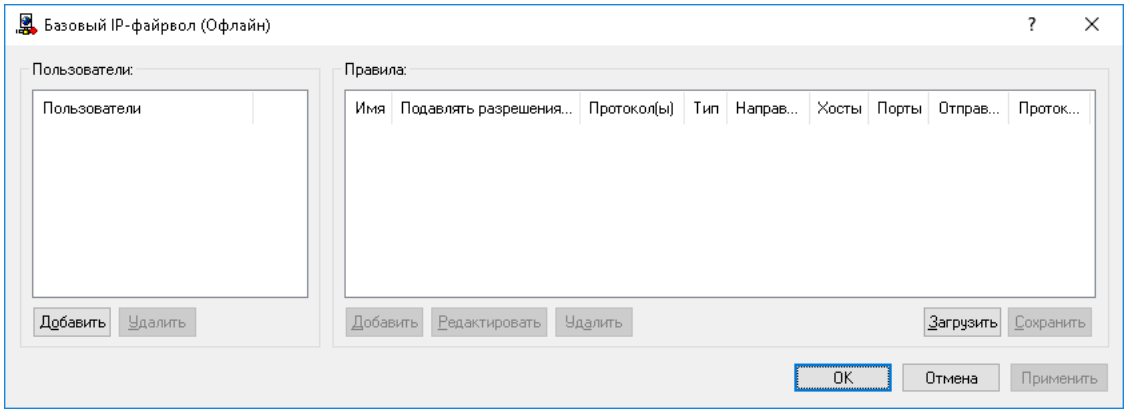
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -
   - Выберите **Базовый IP-файрвол**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

Появится диалоговое окно “Базовый IP-файрвол (Офлайн)”.



4. В левой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

5. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать правило файрвола, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой части диалогового окна “Базовый IP-файрвол (Офлайн)”.

   Чтобы удалить пользователя или группу, в левой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Пользователи**, выберите пользователя или группу, а затем нажмите кнопку **Удалить**.

6. В левой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Пользователи** выберите пользователя или группу.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

7. В правой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Правила** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Добавить правило”.

8. В диалоговом окне **Добавить правило** задайте параметры правила:

   - Чтобы задать имя правила, введите его в поле **Имя**.
   - Чтобы блокировать доступ к узлам, указанным в параметре **Хосты**, установите флажок **Подавлять разрешения протоколов**. Подробнее см. в описании параметра Подавлять разрешения протоколов ранее в этом документе.
   - Чтобы указать протокол, в разделе **Протокол** установите флажок рядом с нужным протоколом. Подробнее см. в описании параметра Протокол ранее в этом документе.
   - Чтобы указать действия, которые файрвол должен выполнять для всех подключений, удовлетворяющих правилу, в области **Тип** выберите один из следующих вариантов: **Разрешение** или **Запрет**. Подробнее см. в описании параметра Тип ранее в этом документе.
   - Чтобы указать направление трафика, к которому применяется правило, в области **Направление** установите соответствующий флажок. Подробнее см. в описании параметра Направление ранее в этом документе.

- Чтобы указать дополнительные действия, которые будут выполняться при срабатывании правила, в области **Если правило срабатывает** установите соответствующий флажок. Подробнее см. в описании параметра Если правило срабатывает ранее в этом документе.
- Чтобы указать удаленные узлы, к которым применяется правило, в поле **Хосты** введите имена узлов или IP-адреса через запятую или точку с запятой. Подробнее см. в описании параметра Хосты ранее в этом документе.
- Чтобы указать порты удаленных узлов, к которым применяется правило, в поле **Порты** введите номера портов через запятую или точку с запятой. Подробнее см. в описании параметра Порты ранее в этом документе.

9. Нажмите кнопку **OK**.

   Созданное правило появится в области "Правила" в правой части диалогового окна "Базовый IP-файрвол (Офлайн)".

10. Нажмите кнопку **OK** или **Применить**.

    Пользователи и группы, для которых заданы правила файрвола, отображаются в дереве консоли в узле "Базовый IP-файрвол".

Если в дереве консоли выбрать пользователя или группу, для которой задано правило файрвола, на панели сведений отобразится информация о заданном правиле (подробнее см. в разделе Правила файрвола).

Можно задавать правила файрвола для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Для получения информации о том, как задать правила файрвола для оперативного режима, см. раздел Базовый IP-файрвол.

Редактирование правил файрвола

Можно изменять значения параметров, настроенных для автономного правила файрвола, в любое время.

Чтобы отредактировать автономное правило файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock с заданными политиками DeviceLock для автономного режима.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** щелкните правой кнопкой мыши **Базовый IP-файрвол**, выберите команду **Управление офлайновыми настройками**, а затем выполните следующие действия:

   a) В левой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Пользователи**, выберите пользователя или группу, для которого требуется изменить правило.

      Если выбрать пользователей или группы, в области "Правила" в правой части диалогового окна отобразятся правила файрвола, которые применяются к этим пользователям или группам.

   b) В правой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Правила** выберите правило, которое требуется редактировать, а затем нажмите кнопку **Редактировать**.

      - или -

      Щелкните правой кнопкой мыши правило, а затем выберите команду **Редактировать**.

   - или -

   В узле **Протоколы** раскройте узел **Базовый IP-файрвол** и выполните следующее:

   a) В узле **Базовый IP-файрвол** выберите пользователя или группу, для которой необходимо изменить правило.

      Если выбрать пользователей или группы, на панели сведений отобразятся правила файрвола, которые применяются к этим пользователям или группам.

   b) На панели сведений щелкните правой кнопкой мыши правило, которое требуется редактировать, а затем выберите команду **Редактировать**.

      - или -

      На панели сведений дважды щелкните правило, которое требуется редактировать.

   Появится диалоговое окно "Редактирование правила".

4. В диалоговом окне **Редактирование правила** внесите необходимые изменения.
5. Нажмите кнопку **OK**, чтобы применить изменения.

Копирование правил файрвола

Можно выполнять операции вырезать-вставить, копировать-вставить, а также операции перетаскивания, чтобы повторно использовать существующие автономные правила файрвола.

Чтобы скопировать автономное правило файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock с заданными политиками DeviceLock для автономного режима.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -

   - Выберите **Базовый IP-файрвол**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

   Появится диалоговое окно "Базовый IP-файрвол (Офлайн)".

4. В левой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Пользователи** выберите пользователя или группу, к которой применяется правило, которое требуется скопировать.

   Если выбрать пользователей или группы, в области "Правила" в правой части диалогового окна отобразятся правила файрвола, которые применяются к этим пользователям или группам.

5. В правой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Правила** щелкните правой кнопкой мыши правило, которое требуется скопировать, а затем выберите команду **Копировать** или **Вырезать**.

   Вырезанное или скопированное правило автоматически копируется в буфер обмена.

   Также можно использовать сочетания клавиш CTRL+C, CTRL+X и CTRL+V, чтобы скопировать, вырезать и вставить правило. При нажатии CTRL+X правило будет вырезано только после того, как вы его вставите.

   Можно одновременно скопировать и вставить сразу несколько правил. Для этого удерживая клавишу SHIFT или CTRL, последовательно выберите каждое правило, затем щелкните их правой кнопкой мыши и выберите **Копировать**.

6. В левой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

7. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых должно применяться скопированное правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой части диалогового окна “Базовый IP-файрвол (Офлайн)”.

8. В левой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Пользователи** выберите пользователей или группы, для которых требуется задать скопированное правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

9. В правой части диалогового окна **Базовый IP-файрвол (Офлайн)** щелкните правой кнопкой мыши в области **Правила**, а затем выберите команду **Вставить**.

   Скопированное правило появится в области “Правила” в правой части диалогового окна “Базовый IP-файрвол (Офлайн)”.

10. Нажмите кнопку **OK** или **Применить**, чтобы применить скопированное правило.

Экспорт и импорт правил файрвола

Можно экспортировать все автономные правила файрвола в файл с расширением .ipp, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт правил также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать автономные правила файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock с заданными политиками DeviceLock для автономного режима.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Выберите **Базовый IP-файрвол**, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши любого пользователя или группу в правиле файрвола. На панели сведений щелкните правой кнопкой правило файрвола, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Раскройте **Базовый IP-файрвол**, выберите любого пользователя или группу в правиле файрвола, а затем щелкните **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление офлайновыми настройками**. В правой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Правила** нажмите кнопку **Сохранить**.
4. В появившемся диалоговом окне выберите папку, в которую требуется сохранить файл, задайте имя файла, и нажмите кнопку **Сохранить**.

   Экспортированные автономные правила сохраняются в файле с расширением .ipp.

Чтобы импортировать автономные правила файрвола

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -
   - Выберите **Базовый IP-файрвол**, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -
   - Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши любого пользователя или группу, указанную в белом списке, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -
   - Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши любого пользователя или группу в правиле файрвола. На панели сведений щелкните правой кнопкой правило файрвола, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -
   - Раскройте **Базовый IP-файрвол**, выберите любого пользователя или группу в правиле файрвола, а затем щелкните **Загрузить офлайновые настройки** на панели инструментов.

     - или -
   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление офлайновыми настройками**. В правой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Правила** нажмите кнопку **Загрузить**.
4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

   Если автономные правила файрвола уже настроены и вы импортируете новые правила, появится следующее сообщение: "Вы хотите перезаписать существующие записи (Да - перезаписать, Нет - добавить)?" В окне сообщения нажмите кнопку "Да", чтобы перезаписать существующие автономные правила файрвола. Нажмите кнопку "Нет", чтобы добавить новые автономные правила файрвола к существующим.

Удаление отдельных правил файрвола

Можно удалить отдельные правила файрвола для автономного режима, если они больше не нужны.

Чтобы удалить правило файрвола для автономного режима

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock с заданными политиками DeviceLock для автономного режима.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Раскройте **Базовый IP-файрвол**, щелкните правой кнопкой мыши пользователя или группу, для которой задано правило, а затем выберите команду **Удалить пользователя**.

     Если удалить пользователя или группу, все правила, заданные для этого пользователя или группы, автоматически удалятся.

     - или -

   - Раскройте **Базовый IP-файрвол**, затем выберите пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, заданное для этого пользователя или группы, а затем выберите команду **Удалить**.

     - или -

   - Щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление офлайновыми настройками**. В левой части диалогового окна **Базовый IP-файрвол (Офлайн)** в области **Пользователи** выберите пользователя или группу, для которой задано правило. В правой части диалогового окна в области **Правила** выберите правило и затем нажмите кнопку **Удалить** или щелкните правой кнопкой мыши правило и затем выберите команду **Удалить**.

Сброс правил файрвола

Можно вернуть ранее заданные правила файрвола для автономного режима в исходное "неопределенное" состояние. Если правила для автономного режима находятся в исходном "неопределенном" состоянии, к клиентским компьютерам, работающим автономно, применяются правила для оперативного режима.

Чтобы сбросить правила файрвола для автономного режима

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock с заданными политиками DeviceLock для автономного режима.

   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние файрвола для автономного режима изменится на "Не задано".

   Если в дереве консоли выбрать **Базовый IP-файрвол**, на панели сведений выводится следующее сообщение: "Офлайновый IP-файрвол не задан."

Удаление всех правил файрвола, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование правил файрвола для автономного режима от объектов более высокого уровня и принудительно применять правила файрвола для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение правил файрвола для оперативного режима, необходимо удалить правила для автономного режима.

Чтобы удалить все автономные правила файрвола

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние файрвола для автономного режима изменится на "Использовать обычный".

   Если в дереве консоли выбрать **Базовый IP-файрвол**, на панели сведений выводится следующее сообщение: "Офлайновый IP-файрвол использует конфигурацию обычного IP-файрвола."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление контентно-зависимыми правилами

Подробное описание функциональности контентно-зависимых правил для протоколов см. в разделе Правила для протоколов главы Контентно-зависимые правила (обычный профиль).

Контентно-зависимые правила для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - Контентно-зависимые правила не заданы. Содержит следующее сообщение: "Офлайновые контентно-зависимые правила не заданы." Это состояние отображается по умолчанию.
- **Задано** - Контентно-зависимые правила заданы.
- **Использовать обычный** - Наследование контентно-зависимых правил для автономного режима блокируется и принудительно применяются контентно-зависимые правила для оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение контентно-зависимых правил для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование контентно-зависимых правил для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении контентно-зависимых правил для оперативного режима см. в разделе Удаление всех контентно-зависимых правил, заданных для автономного режима.

Управление контентно-зависимыми правилами для автономного режима предполагает:

- Создание контентно-зависимых правил
- Редактирование контентно-зависимых правил
- Сброс контентно-зависимых правил
- Экспорт и импорт контентно-зависимых правил
- Удаление отдельных контентно-зависимых правил
- Сброс контентно-зависимых правил
- Удаление всех контентно-зависимых правил, заданных для автономного режима

Создание контентно-зависимых правил

Контентно-зависимые правила создаются на основе встроенных или пользовательских контентных групп. Подробную информацию об этих группах см. в разделе Настройка контентных групп.

Вы можете включить тревожные оповещения о том, что сработало контентно-зависимое правило. Такие оповещения включаются при настройке контентно-зависимого правила.

DeviceLock рассылает тревожные оповещения с учетом соответствующих настроек. В этих настройках задается адресат и способ отправки оповещений. Перед включением оповещений для контентно-зависимых правил задайте параметры оповещений в настройках сервиса DeviceLock (см. раздел Алерты).

Чтобы создать контентно-зависимое правило

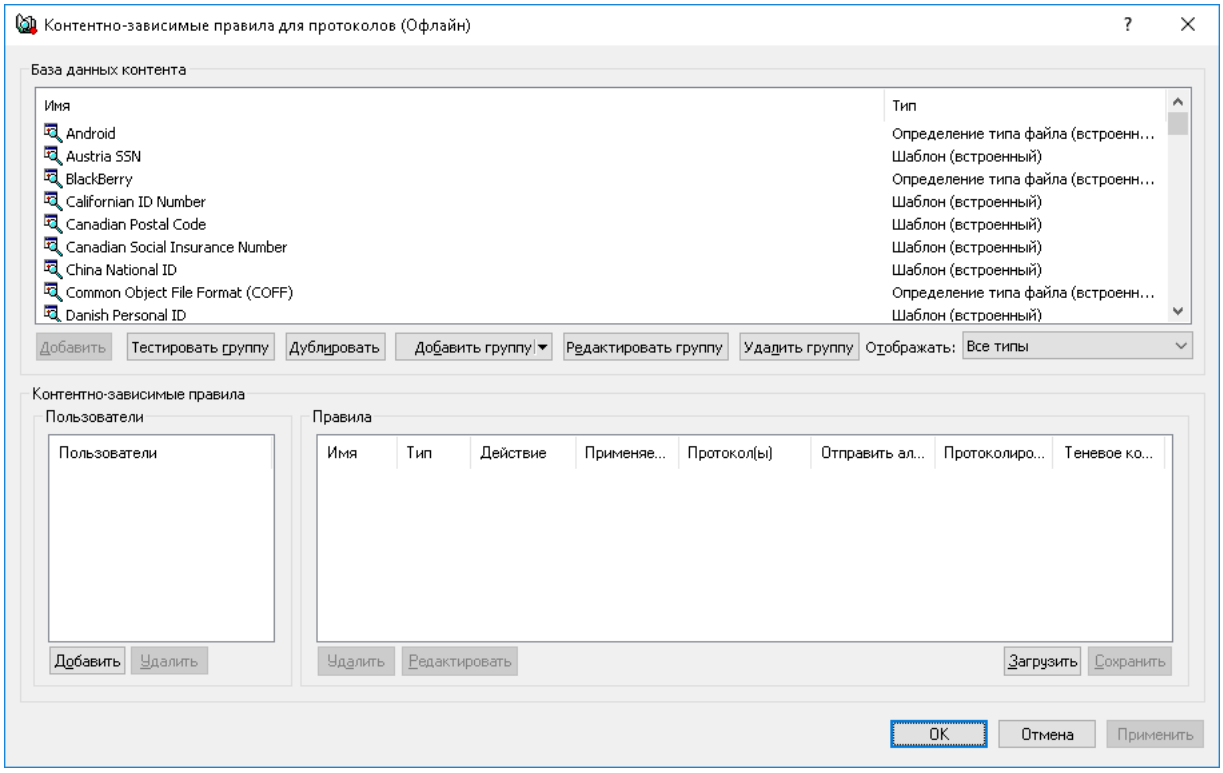
1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

Появится диалоговое окно “Контентно-зависимые правила для протоколов (Офлайн)”.



4. В левой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

   Появится диалоговое окно “Выбор: "Пользователи" или "Группы"”.

5. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых требуется задать правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области “Пользователи” в левой нижней части диалогового окна “Контентно-зависимые правила для протоколов (Офлайн)”.

   Чтобы удалить пользователя или группу, в области **Пользователи** в левой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** выберите пользователя или группу, а затем нажмите кнопку **Удалить** или нажмите клавишу DELETE.

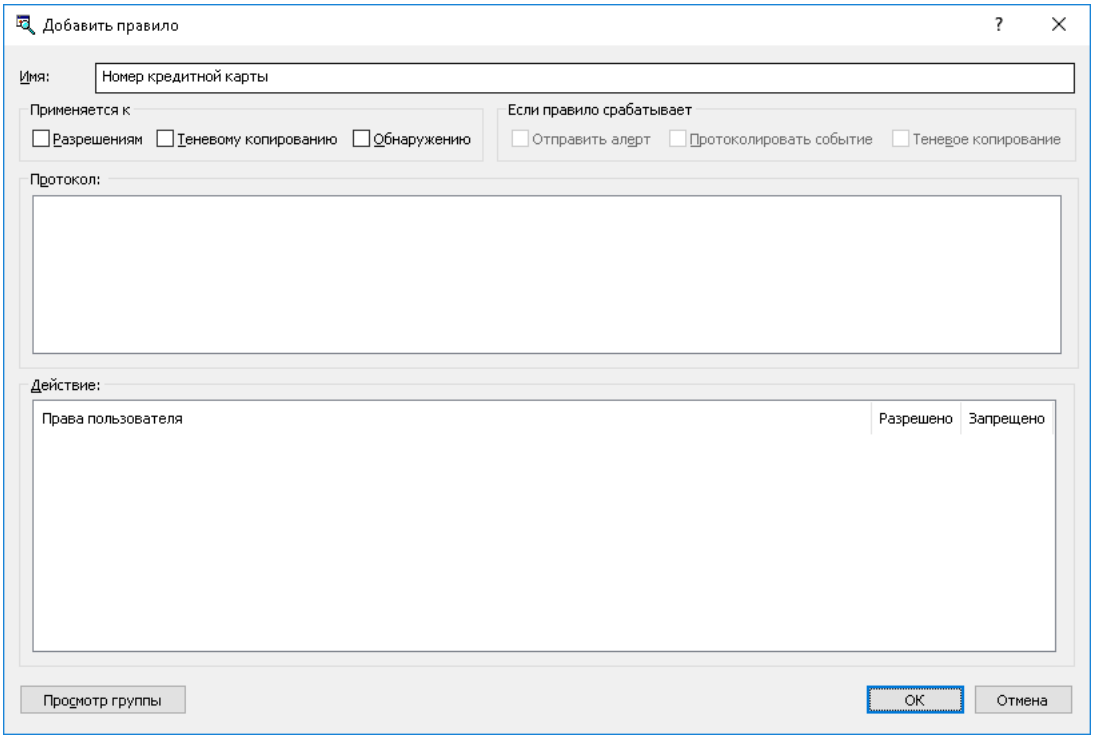
6. В левой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Пользователи** выберите пользователя или группу, для которой требуется задать правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

7. В верхней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **База данных контента** выберите необходимую контентную группу, а затем нажмите кнопку **Добавить**, или дважды щелкните необходимую контентную группу.

   Примечание: Для каждого создаваемого контентно-зависимого правила можно указать только одну контентную группу.

Появится диалоговое окно “Добавить правило”.



8. В диалоговом окне **Добавить правило** в поле **Имя** введите имя контентно-зависимого правила.

   Имя правила по умолчанию совпадает с именем его контентной группы. При необходимости имя правила может быть изменено.

   Для просмотра контентной группы данного правила нажмите кнопку **Просмотр группы** в левом нижнем углу диалогового окна. Консоль отображает свойства группы в отдельном диалоговом окне, позволяя просматривать свойства, но не изменять их.

9. В области **Применяется к** укажите тип операций, к которым должно применяться это правило. Возможные варианты:

   - **Разрешениям** - Указывает, что правило применяется к операциям контроля доступа.
   - **Теневому копированию** - Указывает, что правило применяется к операциям теневого копирования.
   - **Обнаружению** - Указывает, что правило будет обнаруживать указанное содержимое передаваемых данных, при этом будут протоколироваться события обнаружения и отправляться тревожные уведомления, если установлены соответствующие флаги.
   - **Разрешениям**, **Теневому копированию** - Указывает, что правило применяется и к операциям контроля доступа, и к операциям теневого копирования.
   - **Разрешениям, Обнаружению** - Указывает, что правило будет применяться как для операция контроля, так и для операций обнаружения.
   - **Теневому копированию, Обнаружению** - Указывает, что правило будет применяться как для операций избирательного теневого копирования, так и для операций обнаружения.
   - **Разрешениям, Теневому копированию, Обнаружению** - Указывает, что правило будет применяться как для операций контроля и избирательного теневого копирования, так и для операций обнаружения.

Примечание: Для успешного создания/сохранения правила, применяемого исключительно к операциям обнаружения или же к к операциям обнаружения в совокупности с другими операциями, необходимо установить по крайней мере один из флажков: **Протоколировать событие**, **Отправить алерт** или **Теневое копирование** (см. шаг 10 этой процедуры). В противном случае, такое правило не сохраняется, и появляется следующее сообщение: "Необходимо выбрать флаг Протоколировать событие, Отправить алерт или Теневое копирование."

10. В области **Если правило срабатывает** укажите следующие дополнительные операции, которые будут выполняться при срабатывании правила:

    - **Отправить алерт** - Оповещение рассылается при каждом срабатывании правила.
    - **Протоколировать событие** - Событие регистрируется в журнале аудита при каждом срабатывании правила.
    - **Теневое копирование** - Теневая копия данных создается при каждом срабатывании правила.

    При включении или отключении алертов, аудита и/или теневого копирования в контентно-зависимом правиле настройка правила имеет приоритет над соответствующей настройкой для протокола.

    Пример: Если аудит включен для некоторого протокола и отключен в правиле для этого протокола, срабатывание такого правила не вызовет события аудита. Если же аудит в правиле включен, то срабатывание правила вызовет событие аудита, даже если аудит отключен на уровне протокола.

    Правило может наследовать настройку алертов, аудита и/или теневого копирования, заданную на уровне протокола. Эта опция выбрана по умолчанию и представлена неопределенным состоянием флажков (не установленных и не очищенных). Состояние каждого флажка можно изменить независимо от других.

    Пример: Если правило наследует настройку аудита, заданную для протокола, то срабатывание такого правила вызовет событие аудита только если аудит включен для протокола, контролируемого этим правилом.

11. В области **Протокол** выберите протоколы, к которым должно применяться это правило.

    Контентно-зависимые правила могут применяться к следующим протоколам: Поиск работы, Файловые хранилища, FTP, HTTP, IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMB, SMTP, Социальные сети, Telegram, Viber, Web-почта, Web-поиск, WhatsApp и Zoom.

    Если выбраны различные протоколы, имеющие разные наборы возможных прав доступа, в области "Действие" диалогового окна будут показаны все действия, применимые для каждого из выбранных протоколов. В результирующем правиле эффективными будут только те действия, которые применимы для конкретного протокола.

12. В области **Действие** укажите, какие действия с протоколами пользователю разрешены или запрещены, какие действия пользователя будут записываться в журнале теневого копирования, а также какие действия пользователя будут трактоваться как события обнаружения содержимого.

    О правах, которые могут быть заданы в контентно-зависимых правилах, см. Управление доступом к контенту, Теневое копирование контента и Обнаружение контента для протоколов.

13. Нажмите кнопку **OK**.

    Созданное правило отображается в области "Правила" в правой нижней части диалогового окна "Контентно-зависимые правила для протоколов (Офлайн)".

14. Нажмите кнопку **OK** или **Применить**, чтобы применить правило.

Пользователи и группы, для которых заданы контентно-зависимые правила, отображаются в дереве консоли в узле **Контентно-зависимые правила** для протоколов. Если в дереве консоли выбрать пользователя или группу, для которой задано правило, на панели сведений отобразится информация о заданном правиле (подробнее см. в разделе Список контентно-зависимых правил для протоколов).

Можно задавать контентно-зависимые правила для разных режимов работы (оперативного и автономного) для одних и тех же пользователей или групп. Для получения информации о том, как задать контентно-зависимые правила для оперативного режима, см. раздел Управление контентно-зависимыми правилами в главе Контентно-зависимые правила (обычный профиль).

Редактирование контентно-зависимых правил

Можно редактировать свойства заданных контентно-зависимых правил, такие как **Имя**, **Применяется к**, **Если правило срабатывает, Протокол, Действие**.

Чтобы редактировать контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** щелкните правой кнопкой мыши **Контентно-зависимые правила**, выберите команду **Управление офлайновыми настройками**, а затем выполните следующее:
   a) В левой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Пользователи** выберите пользователя или группу, для которой задано правило, которое требуется редактировать.

      Если выбрать пользователей или группы, в области "Правила" в правой нижней части диалогового окна отображаются контентно-зависимые правила, которые применяются к этим пользователям или группам.
   b) В правой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Rules** выберите правило, которое требуется редактировать, а затем нажмите кнопку **Редактировать**.

      - или -

      Щелкните правой кнопкой мыши правило, а затем выберите команду **Редактировать**.

      - или -

      Дважды щелкните правило.

- или -

В узле **Протоколы** раскройте узел **Контентно-зависимые правила**, а затем выполните следующее:

a) В узле **Контентно-зависимые правила** выберите пользователя или группу, для которой требуется редактировать правило.

b) На панели сведений щелкните правой кнопкой мыши правило, которое требуется редактировать, а затем выберите команду **Редактировать**.

- или -

На панели сведений дважды щелкните правило, которое требуется редактировать.

Появится диалоговое окно "Редактирование правила".

4. В диалоговом окне **Редактирование правила** внесите необходимые изменения.
5. Нажмите кнопку **OK**, чтобы применить изменения.

Копирование контентно-зависимых правил

Можно выполнять операции вырезать-вставить, копировать-вставить, а также операции перетаскивания, чтобы повторно использовать существующие контентно-зависимые правила для автономного режима.

Чтобы скопировать контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**.

     - или -

   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Управление офлайновыми настройками** на панели инструментов.

   Появится диалоговое окно "Контентно-зависимые правила для протоколов (Офлайн)".

4. В левой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Пользователи** выберите пользователя или группу, к которой применяется правило, которое требуется скопировать.

   Если выбрать пользователей или группы, в области "Правила" в правой нижней части диалогового окна отображаются контентно-зависимые правила, которые применяются к этим пользователям или группам.

5. В правой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Правила** щелкните правой кнопкой мыши правило, которое требуется скопировать, а затем выберите команду **Копировать** или **Вырезать**.

   Вырезанное или скопированное правило автоматически копируется в буфер обмена.

   Также можно использовать сочетания клавиш CTRL+C, CTRL+X и CTRL+V, чтобы скопировать, вырезать и вставить правило. При нажатии CTRL+X правило будет вырезано только после того, как вы его вставите.

   Для выполнения операции перетаскивания выделите правило и перетащите его к пользователю или группе, к которой требуется применить скопированное правило.

6. В левой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Пользователи** нажмите кнопку **Добавить**.

7. В появившемся диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имена пользователей или групп, для которых должно применяться скопированное правило, а затем нажмите кнопку **OK**.

   Добавленные пользователи и группы отображаются в области "Пользователи" в левой нижней части диалогового окна "Контентно-зависимые правила для протоколов (Офлайн)".

8. В левой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Пользователи** выберите пользователей или группы, для которых требуется задать скопированное правило.

   Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

9. В правой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** щелкните правой кнопкой мыши в области **Правила**, а затем выберите команду **Вставить**.

   Скопированное правило отображается в области "Правила" в правой нижней части диалогового окна "Контентно-зависимые правила для протоколов (Офлайн)".

10. Нажмите кнопку **OK** или **Применить**, чтобы применить скопированное правило.

Экспорт и импорт контентно-зависимых правил

Можно экспортировать все заданные контентно-зависимые правила для автономного режима в файл с расширением .cwl, а затем импортировать его и использовать на другом компьютере. Экспорт и импорт правил также могут быть использованы как вариант резервного копирования.

Чтобы экспортировать контентно-зависимые правила

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши любого пользователя или группу, для которой задано правило, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой правило, а затем выберите команду **Сохранить офлайновые настройки**.

     - или -
   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило, а затем щелкните значок **Сохранить офлайновые настройки** на панели инструментов.

     - или -
   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**. В правой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Правила** нажмите кнопку **Сохранить**.
4. В появившемся диалоговом окне выберите папку, в которую требуется сохранить файл, задайте имя файла, и нажмите кнопку **Сохранить**.

   При экспорте правила сохраняются в файле с расширением .cwl.

Чтобы импортировать контентно-зависимые правила

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Выберите **Контентно-зависимые правила**, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -

   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши любого пользователя или группу, для которой задано правило, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, а затем выберите команду **Загрузить офлайновые настройки**.

     - или -

   - Раскройте **Контентно-зависимые правила**, выберите любого пользователя или группу, для которой задано правило, а затем щелкните значок **Загрузить офлайновые настройки** на панели инструментов.

     - или -

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**. В правой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Правила** нажмите кнопку **Загрузить**.

4. В появившемся диалоговом окне найдите и выберите файл, который требуется импортировать, а затем нажмите кнопку **Открыть**.

   За один раз можно импортировать только один файл .cwl.

Удаление отдельных контентно-зависимых правил

Можно удалять отдельные контентно-зависимые правила для автономного режима, если они больше не нужны.

Чтобы удалить отдельное контентно-зависимое правило

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Раскройте **Контентно-зависимые правила**, щелкните правой кнопкой мыши пользователя или группу, для которой задано правило, а затем выберите команду **Удалить пользователя**.

     Если удалить пользователя или группу, все правила, заданные для этого пользователя или группы, автоматически удалятся.

     - или -

   - Раскройте **Контентно-зависимые правила**, затем выберите пользователя или группу, для которой задано правило. На панели сведений щелкните правой кнопкой мыши правило, заданное для этого пользователя или группы, а затем выберите команду **Удалить**.

     - или -

   - Щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление офлайновыми настройками**. В левой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Пользователи** выберите пользователя или группу, для которой задано правило. В правой нижней части диалогового окна **Контентно-зависимые правила для протоколов (Офлайн)** в области **Правила** выберите правило и затем нажмите кнопку **Удалить** или щелкните правой кнопкой мыши правило и затем выберите команду **Удалить**.

     Чтобы выбрать одновременно несколько правил, используйте клавиши SHIFT или CTRL.

Сброс контентно-зависимых правил

Можно вернуть ранее заданные контентно-зависимые правила в исходное “неопределенное” состояние. Если правила для автономного режима находятся в исходном “неопределенном” состоянии, к клиентским компьютерам, работающим автономно, применяются правила для оперативного режима.

Чтобы вернуть контентно-зависимые правила в исходное “неопределенное” состояние

1. Если используется консоль DeviceLock Management Console, выполните следующее:
   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Сбросить офлайновые настройки**.

   Состояние контентно-зависимых правил для автономного режима изменится на “Не задано”.

   Если в дереве консоли выбрать **Контентно-зависимые правила**, на панели сведений выводится следующее сообщение: “Офлайновые контентно-зависимые правила не заданы.”

Удаление всех контентно-зависимых правил, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование контентно-зависимых правил для автономного режима от объектов более высокого уровня и принудительно применять контентно-зависимые правила для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение контентно-зависимых правил для оперативного режима, необходимо удалить контентно-зависимые правила для автономного режима.

Чтобы удалить все заданные контентно-зависимые правила

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние контентно-зависимых правил для автономного режима изменится на "Использовать обычный."

   Если в дереве консоли выбрать **Контентно-зависимые правила**, на панели сведений выводится следующее сообщение: "Офлайновые контентно-зависимые правила используют конфигурацию обычных правил."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

Управление настройками безопасности

Подробное описание функциональности настроек безопасности для протоколов см. в разделе Настройки безопасности для протоколов для оперативного режима.

Настройки безопасности для автономного режима могут иметь одно из следующих состояний:

- **Не задано** - Настройки безопасности не заданы для протоколов. Это состояние отображается по умолчанию.
- **Включено** - Настройки безопасности включены для протоколов.
- **Отключено** - Настройки безопасности отключены для протоколов.
- **Использовать обычный** - Наследование настроек безопасности для автономного режима блокируется и принудительно применяются настройки безопасности для оперативного режима. Параметры DeviceLock для автономного режима могут иметь это состояние только в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager.

  Принудительное применение настроек безопасности для оперативного режима полезно при использовании групповой политики или файла настроек сервиса DeviceLock (.dls) для развертывания политик DeviceLock в корпоративной сети, поскольку позволяет предотвратить наследование настроек безопасности для автономного режима от объектов более высокого уровня.

  Подробнее о принудительном применении настроек безопасности для оперативного режима см. в разделе Удаление всех настроек безопасности, заданных для автономного режима.

Управление настройками безопасности для автономного режима предполагает:

- Задание и редактирование настроек безопасности
- Сброс настроек безопасности
- Удаление всех настроек безопасности, заданных для автономного режима

Задание и редактирование настроек безопасности

Чтобы задать и редактировать настройки безопасности

1. Если используется консоль DeviceLock Management Console, выполните следующее:

   a) Откройте DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor, выполните следующее:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:

   a) Откройте Group Policy Object Editor.

   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.

2. Раскройте узел **Протоколы**.

3. В узле **Протоколы** выполните одно из следующих действий:

   - Выберите **Настройки безопасности**. На панели сведений щелкните правой кнопкой мыши нужную настройку безопасности, а затем выберите команду **Включить офлайн** или **Выключить офлайн**.

     Если в дереве консоли выбрать "Настройки безопасности", на панели сведений отобразятся настройки безопасности.

     - или -

   - Щелкните правой кнопкой мыши **Настройки безопасности**, а затем выберите команду **Управление офлайновыми настройками**. В открывшемся диалоговом окне **Настройки безопасности (Офлайн)** установите флажки для настроек безопасности, которые требуется задать, а затем нажмите кнопку **OK**.

     Чтобы открыть диалоговое окно "Настройки безопасности", можно также выбрать "Настройки безопасности" в дереве консоли, а затем щелкнуть значок "Управление офлайновыми настройками" на панели инструментов.

     Примечание: Все флажки в диалоговом окне **Настройки безопасности (Офлайн)** могут иметь одно из трех состояний: установленные, снятые или в неопределенном состоянии, что соответствует состояниям **Включено**, **Отключено** и **Не задано** настроек безопасности.

   Состояние настройки безопасности для автономного режима изменится с "Не задано" на "Включено" или "Отключено".

Сброс настроек безопасности

Можно вернуть ранее заданные настройки безопасности в исходное "неопределенное" состояние. Если настройки для автономного режима находятся в исходном "неопределенном" состоянии, к клиентским компьютерам, работающим автономно, применяются настройки для оперативного режима.

Чтобы вернуть настройки безопасности в исходное "неопределенное" состояние

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock с заданными политиками DeviceLock для автономного режима.
   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выполните одно из следующих действий:
   - Выберите **Настройки безопасности**. На панели сведений щелкните правой кнопкой мыши нужную настройку безопасности, а затем выберите команду **Сбросить офлайновые настройки**.

     Если в дереве консоли выбрать "Настройки безопасности", на панели сведений отобразятся настройки безопасности.

     - или -
   - Щелкните правой кнопкой мыши **Настройки безопасности**, а затем выберите команду **Управление офлайновыми настройками**. В открывшемся диалоговом окне **Настройки безопасности (Офлайн)** задайте неопределенное состояние для настройки безопасности, а затем нажмите кнопку **OK**.

     Чтобы открыть диалоговое окно "Настройки безопасности", можно также выбрать "Настройки безопасности" в дереве консоли, а затем щелкнуть значок "Управление офлайновыми настройками" на панели инструментов.

     Примечание: Все флажки в диалоговом окне **Настройки безопасности (Офлайн)** могут иметь одно из трех состояний: установленные, снятые или в неопределенном состоянии, что соответствует состояниям **Включено**, **Отключено** и **Не задано** настроек безопасности.

   Состояние настройки безопасности для автономного режима изменится на "Не задано".

Удаление всех настроек безопасности, заданных для автономного режима

Для сценариев развертывания политик DeviceLock с помощью групповой политики или файла настроек (.dls) DeviceLock предоставляет возможность блокировать наследование настроек безопасности для автономного режима от объектов более высокого уровня и принудительно применять настройки безопасности для оперативного режима на объектах более низкого уровня. Чтобы обеспечить принудительное применение настроек безопасности для оперативного режима, необходимо удалить настройки безопасности для автономного режима. Настройки безопасности для автономного режима удаляются по отдельности.

Чтобы удалить настройки безопасности

1. Если используется консоль DeviceLock Service Settings Editor, выполните следующее:
   a) Откройте DeviceLock Service Settings Editor.
   b) В дереве консоли щелкните правой кнопкой мыши узел **Настройки DeviceLock** или **Сервис DeviceLock**, а затем выберите **Загрузить настройки сервиса**, чтобы открыть файл настроек сервиса DeviceLock с заданными политиками DeviceLock для автономного режима.
   c) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующее:
   a) Откройте Group Policy Object Editor.
   b) В дереве консоли раскройте узел **Конфигурация компьютера**, а затем раскройте узел **DeviceLock**.
2. Раскройте узел **Протоколы**.
3. В узле **Протоколы** выберите **Настройки безопасности**.

   Если в дереве консоли выбрать "Настройки безопасности", на панели сведений отобразятся настройки безопасности.
4. На панели сведений щелкните правой кнопкой мыши настройку безопасности, которую необходимо удалить, а затем выберите команду **Удалить офлайновые настройки**.

   Состояние настройки безопасности для автономного режима изменится на "Использовать обычный."

   Состояние "Использовать обычный" параметров DeviceLock отображается как "Не задано" в консоли DeviceLock Management Console.

9

Временный белый список

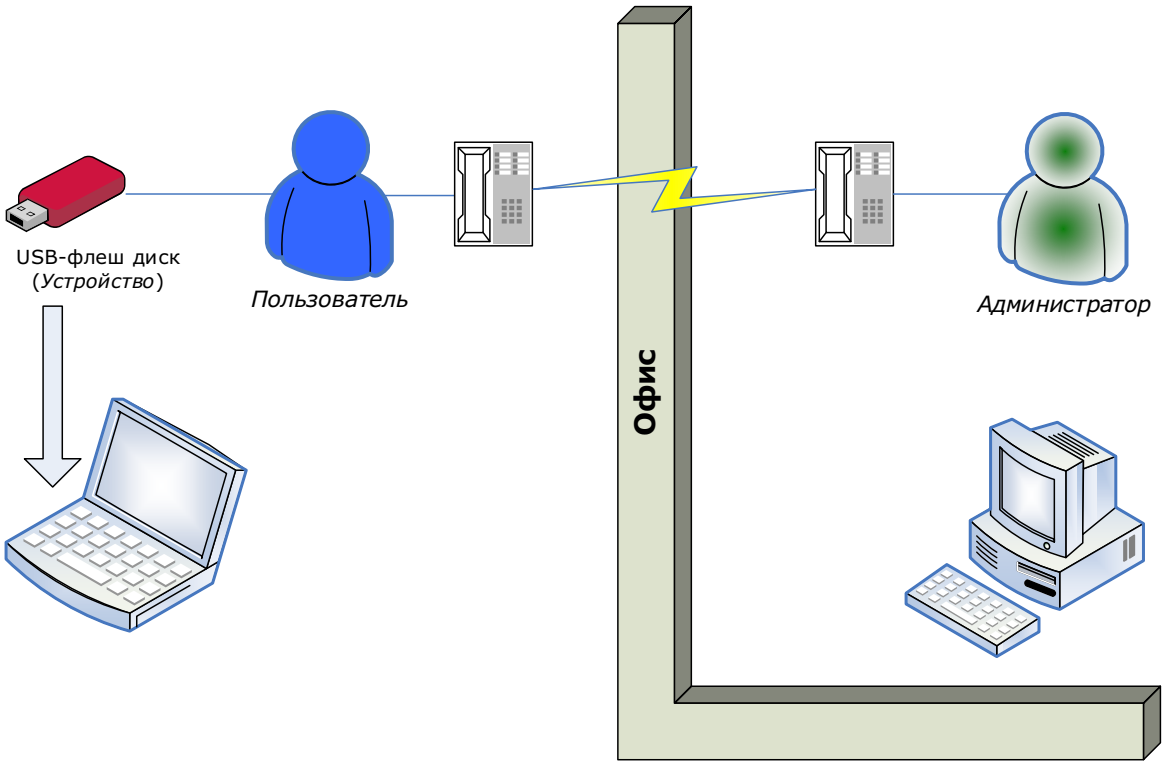
В этой главе:

Общая информация

Получение временного доступа

Общая информация

Функция "Временный белый список" позволяет предоставлять временный доступ к USB-устройствам при отсутствии сетевого подключения. На диаграмме ниже показана процедура предоставления доступа к USB.



Временный белый список функционирует как белый список устройств (см. раздел Белый список USB-устройств (обычный профиль)) за исключением того, что для добавления устройств и предоставления доступа к ним не требуется подключение к сети.

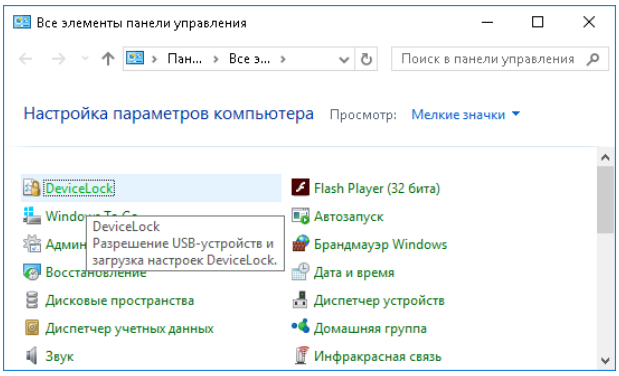
Примечание: Использование временного белого списка - это возможность предоставления доступа к USB-устройствам, которые заблокированы на обоих уровнях: Если находящееся в белом списке устройство (например, USB-накопитель) принадлежит к обоим уровням: интерфейсу (USB) и типу (Съемное устройство), ограничения (если они есть) на уровне типа устройства будут игнорироваться точно так же, как и на уровне USB.

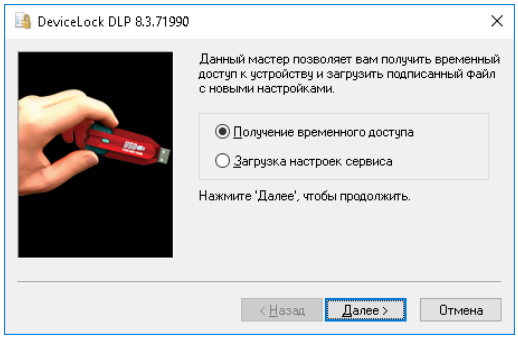
Следующая пошаговая инструкция поможет создать и использовать временный белый список:

1. Администратор создает криптографический сертификат DeviceLock, используя мастер создания сертификата (см. раздел Создание сертификата). Сертификат состоит из двух ключей - секретного (закрытого) и публичного (открытого).
2. Администратор устанавливает сертификат (открытый ключ) на компьютер пользователя. В результате на компьютере пользователя будет включен временный белый список.
3. Когда пользователю необходимо получить доступ к какому-либо USB-устройству, он запускает мастер получения временного доступа (см. Получение временного доступа), выбирает требуемое устройство из списка и формирует буквенно-цифровой код (код устройства). Затем пользователь передает этот код администратору (по телефону или другим способом).
4. Администратор запускает Мастер создания подписи, загружает соответствующий сертификат (секретный ключ), вводит переданный ему код устройства, задает необходимый период времени, формирует ответный код (разблокирующий код), и передает этот код пользователю.
5. Получив разблокирующий код, пользователь вводит его в мастер получения временного доступа (см. Получение временного доступа). Затем пользователю предоставляется доступ к запрошенному устройству на указанный период времени.

Получение временного доступа

Для получения временного доступа к устройству нужно запустить приложение **DeviceLock** из панели управления Windows и выбрать опцию **Получение временного доступа**.



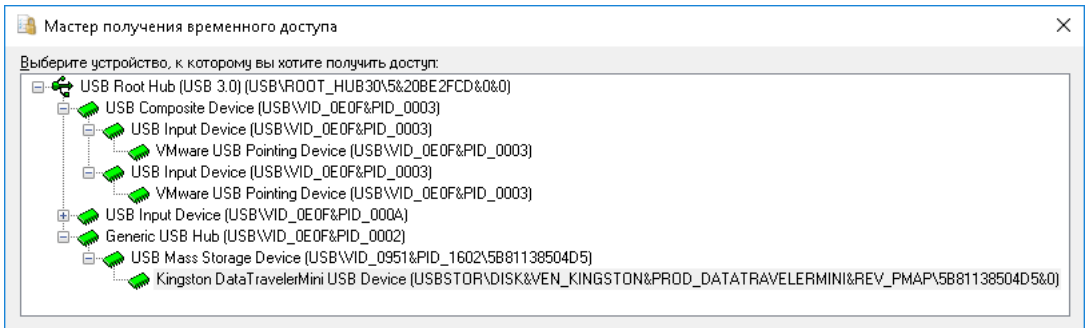


Примечание:

- Для доступа к приложению DeviceLock необходимо выбрать режим просмотра “Мелкие значки” в панели управления.
- В заголовке окна приложения отображаются версия и номер сборки DeviceLock.
- Запуск приложения DeviceLock из панели управления Windows может завершиться ошибкой “Сертификат не установлен.” Для устранения этой проблемы на клиентском компьютере необходимо установить открытый ключ сертификата DeviceLock. Инструкции см. в разделе Установка и удаление сертификата.

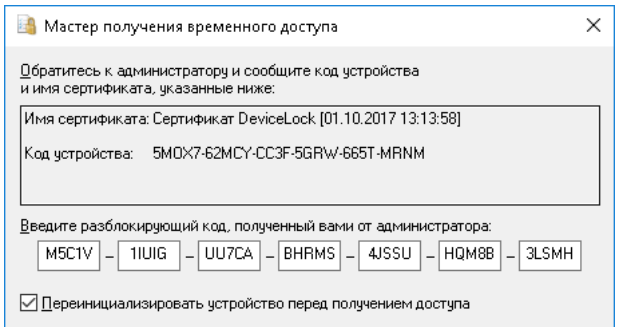
Получение временного доступа к устройству выполняется в пять простых шагов:

1. Подключите требуемое устройство к USB-порту.
2. Выберите устройство из списка доступных USB-устройств и нажмите кнопку **Далее** для перехода к следующей странице мастера.



   Чтобы облегчить выбор нужного устройства, рядом с именем устройства в скобках отображается его PID, VID и серийный номер (при его наличии).

3. Свяжитесь с администратором и передайте ему имя сертификата и код устройства, представленные на следующей странице мастера. Код устройства действителен в течение 24 часов с момента его создания.



4. Введите разблокирующий код, полученный от администратора.

   Если доступ к устройству требует его повторной инициализации (переподключения), установите флажок **Переинициализировать устройство перед получением доступа**. Доступ к некоторым USB-устройствам (таким как мышь) не может быть предоставлен без переподключения, поэтому рекомендуется установить этот флажок для устройств, не предназначенных для хранения данных. Также рекомендуется снять этот флажок для устройств хранения данных (флеш-накопители, оптические приводы, внешние жесткие диски и т.п.).

   Внимание: DeviceLock не может переинициализировать USB-устройства, драйверы которых не позволяют выполнять программное переподключение. При отсутствии доступа к такому устройству необходимо извлечь его из USB-порта и затем вставить обратно для перезапуска драйвера.

5. Нажмите на кнопку **Готово**.

Если пользователь ввел действительный код, доступ к устройству будет предоставлен через несколько секунд. Появится следующее сообщение: “Устройство успешно разблокировано на `<период времени>`.”

Все успешные попытки добавить устройство во временный белый список протоколируются, если включено протоколирование изменений в настройках сервиса DeviceLock (см. описание параметра Записывать события об изменении политики и старте/остановке сервиса).

10

Мониторинг активности пользователей

В этой главе:

Общие сведения

Настройки мониторинга

Просмотр активности пользователей

Общие сведения

DeviceLock предоставляет возможность мониторинга действий пользователя посредством таких инструментов, как видеозапись экрана компьютера, запись нажатий клавиш на клавиатуре, информация о процессах и приложениях, которые работали во время записи. Такие виды мониторинга позволяют существенно расширить доказательную базу при расследовании инцидентов информационной безопасности, а также помогают выявлять подозрительное поведение пользователей и злоупотребления привилегиями доступа или политиками защиты данных, что в результате приводит к снижению рисков утечки данных.

Для осуществления мониторинга активности пользователей сервис DeviceLock записывает в видео формате действия, происходящие на экране пользовательского компьютера, а также выполняет запись того, какие клавиши нажимает пользователь на клавиатуре, и сохраняет дополнительные сведения, такие как имя активного приложения, заголовок активного окна и т.д. Имеется возможность сбора данных с пользовательских компьютеров на сервер DeviceLock Enterprise Server, где уполномоченные лица могут просматривать и анализировать записи активности пользователей.

Возможность записи действий пользователя дает ряд преимуществ при обнаружении угроз утечки данных. Сервис DeviceLock записывает в точности то, что пользователь видит на экране компьютера, независимо от используемых приложений и протоколов или уровня привилегий пользователя. Ввод с клавиатуры и другие данные, записанные сервисом DeviceLock вместе с видео, могут быть использованы для отслеживания определенных действий пользователя.

Сервис DeviceLock предусматривает различные критерии запуска, позволяющие начинать запись при наступлении определенных событий или условий. В зависимости от выбранного критерия запись может начинаться, например, при подключении определенного устройства, запуске некоторого приложения или несанкционированной попытке записи файла или передачи сообщения. Критерии запуска позволяют сервису DeviceLock выполнять выборочную запись вызывающих подозрения действий пользователя. Полный список критериев см. в разделе Настройка критериев запуска далее в этой главе.

Данные мониторинга активности пользователей первоначально сохраняются на локальном компьютере, что позволяет просматривать локальные записи пользовательских действий в консоли DeviceLock Management Console, подключенной к сервису DeviceLock. Так можно просматривать только записи, выполненные сервисом DeviceLock на локальном компьютере.

Для централизованного просмотра и анализа записей с различных компьютеров необходимо передать данные мониторинга активности пользователей на сервер DeviceLock Enterprise Server. Серверы для сбора и хранения данных задаются соответствующим параметром сервиса DeviceLock. При необходимости данные с разных серверов можно объединить для просмотра и анализа на центральном сервере, используя консолидацию журналов.

Приступая к работе с мониторингом активности пользователей

Чтобы использовать мониторинг активности пользователей, администратор DeviceLock должен сначала настроить правила, по которым сервис DeviceLock начинает запись определенных действий пользователя. Для управления этими правилами служат команды узла **Мониторинг активности пользователей** > **Правила** в подключенной к сервису DeviceLock консоли DeviceLock Management Console, либо в консоли DeviceLock Service Settings Editor или DeviceLock Group Policy Manager. Команда **Управление** из контекстного меню узла **Правила** открывает диалоговое окно настройки правила, где требуется:

1. Выбрать пользователей и/или группы, к которым будет применяться правило. Запись активности этих пользователей или групп начинается при выполнении условий срабатывания данного правила.
2. Добавить в правило один или несколько критериев запуска. Добавленные в правило критерии совместно определяют условия, при которых запускается запись активности пользователя.

Подробнее см. в разделе Создание правил далее в этой главе.

Данные мониторинга, собранные сервисом DeviceLock, изначально хранятся на локальном компьютере, что позволяет просматривать локальные записи активности пользователей в подключенной к сервису DeviceLock консоли DeviceLock Management Console, используя узел **Сервис DeviceLock** > **Мониторинг активности пользователей** > **Просмотрщик журнала активности пользователей**.

Внимание: Сервис DeviceLock может приостановить мониторинг активности пользователей из-за недостатка дискового пространства в локальном хранилище данных. Подробнее см. в разделе Квота локального хранилища данных.

Для централизованного просмотра и анализа записей с различных компьютеров необходимо передать данные мониторинга активности пользователей на сервер DeviceLock Enterprise Server. Эти серверы должны быть заданы параметром DeviceLock Enterprise Server(ы) сервиса DeviceLock. Кроме того, для параметра Отправлять данные теневого копирования на сервер необходимо выбрать вариант настройки **Включить**.

Для просмотра записей на сервере DeviceLock Enterprise Server используется узел **DeviceLock Enterprise Server** > **Просмотрщик журнала активности пользователей** в консоли DeviceLock Management Console, подключенной к серверу DeviceLock Enterprise Server. Консоль отображает список всех имеющихся на сервере записей активности пользователей, предоставляя уполномоченным лицам возможность просматривать видеозаписи компьютерных экранов, записи ввода с клавиатуры и другие данные о действиях пользователей. Подробнее см. в разделе Просмотр активности пользователей далее в этой главе.

Настройки мониторинга

Настройки сервиса DeviceLock, относящиеся к мониторингу активности пользователей, представлены в консолях DeviceLock Management Console, DeviceLock Service Settings Editor или DeviceLock Group Policy Manager под узлом **Мониторинг активности пользователей**:

- Параметры - Настройки, общие для всех сеансов записи. Определяют, например, записывать ли цветное или только черно-белое видео.
- Правила - Условия начала/прекращения записи и другие настройки, которые могут различаться для разных сеансов записи. См. также Примеры правил мониторинга активности пользователей.

Внимание: Для мониторинга активности пользователей требуется лицензия DeviceLock UAM в дополнение к основной лицензии DeviceLock. Инструкции по установке лицензии см. в разделе Активация лицензий DeviceLock.

Параметры

Параметры мониторинга активности пользователей - это общие настройки, не зависящие от условий начала/прекращения записи и других настроек, задаваемых правилами мониторинга пользовательской активности. Они отображаются на панели сведений, если в дереве консоли DeviceLock Management Console или DeviceLock Service Settings Editor выбрать **Сервис DeviceLock** > **Мониторинг активности пользователей** > **Параметры**, или если выбрать **DeviceLock** > **Мониторинг активности пользователей** > **Параметры** при использовании консоли DeviceLock Group Policy Manager.

Предусмотрены следующие общие настройки:

- Полутоновое изображение - Определяет, будет ли выполняться черно-белая или цветная запись.
- Приостановить запись при неактивности - Определяет, следует ли приостанавливать запись, когда компьютер не используется.
- Разрешение видео - Определяет разрешение записанного видео.
- Несколько дисплеев - Определяет способ записи экрана на компьютерах, у которых имеется несколько мониторов.
- Логирование паролей - Определяет, записывать ли введенные пользователем пароли открытым текстом или заменять их звездочками.

Полутоновое изображение

Параметр **Полутоновое изображение** определяет цветовой режим записи. Включите этот параметр, чтобы использовать черно-белую запись. Такая запись потребляет меньше ресурсов компьютера и создает меньший объем данных мониторинга. Если требуется цветная запись, отключите этот параметр.

Приостановить запись при неактивности

Параметр **Приостановить запись при неактивности** дает возможность приостанавливать запись при отсутствии активности пользователя, сокращая объем данных мониторинга. Когда этот параметр включен, запись приостанавливается, если пользователь в течение некоторого времени не нажимает клавиши на клавиатуре, не перемещает мышь и не нажимает на нее. Запись возобновляется при нажатии любой клавиши или при нажатии/перемещении мыши. Значение параметра задает максимально допустимое время отсутствия активности.

Дважды щелкните параметр, чтобы просмотреть или изменить его значение в появившемся диалоговом окне:

- **Время неактивности** - Максимальный промежуток времени (число секунд), в течение которого сеанс работы на компьютере может простаивать без действий пользователя, прежде чем запись сеанса будет приостановлена. Сервис DeviceLock автоматически приостанавливает запись неактивных сеансов по истечении заданного количества секунд.

Чтобы включить этот параметр, установите его в ненулевое значение. Допустимое значение составляет `3` или более секунд. Для отключения параметра установите его значение в `0`. Когда параметр отключен, запись продолжается даже при отсутствии активности пользователя.

Примечание: Данный параметр не действует на правила, содержащие критерий запуска `Компьютер простаивает <число> сек.` (см. Настройка критериев запуска). Такие правила не приостанавливают запись по истечении заданного этим параметром времени отсутствия активности пользователя.

Разрешение видео

Параметр **Разрешение видео** позволяет задать выходное разрешение для видеозаписи экрана, сделанной сервисом DeviceLock. Это может быть разрешение записываемого экрана или другое разрешение, выбранное из списка в настройке параметра.

Дважды щелкните параметр, чтобы просмотреть или изменить его настройку в появившемся диалоговом окне:

- **Разрешение** - Выберите желаемое выходное разрешение в раскрывающемся списке для настройки этого параметра.

Чтобы выходное разрешение соответствовало разрешению записываемого экрана, выберите пункт **Базовое** в списке **Разрешение**.

Внимание: При записи сохраняется соотношение сторон записываемого экрана, поэтому высота или ширина полученной видеозаписи может отличаться от задаваемой выходным разрешением. Как правило, ширина совпадает с заданной выходным разрешением, а высота вычисляется так, чтобы сохранить исходное соотношение сторон экрана.

Несколько дисплеев

Параметр **Несколько дисплеев** применяется к компьютерам, у которых имеется более одного монитора, и позволяет указать, следует ли записывать экран только одного монитора или экраны всех мониторов. В последнем случае есть возможность объединить все мониторы в одну запись или записывать каждый монитор отдельно.

Дважды щелкните этот параметр, чтобы просмотреть или изменить выбор его настройки в появившемся диалоговом окне:

- **Только основной монитор** - Записывается только экран основного монитора.
- **Все мониторы в один файл** - Экраны всех мониторов записываются в единую запись.
- **Каждый монитор в отдельный файл** - Записываются экраны всех мониторов, для каждого экрана выполняется отдельная запись.

Логирование паролей

Параметр **Логирование паролей** позволяет при записи нажатий на клавиши защитить вводимые пользователем пароли, заменяя их звездочками (*).

Включите этот параметр, если допускается запись паролей. В результате пароли записываются открытым текстом, который будет отображен и выделен красным при просмотре записи. Чтобы избежать записи паролей, отключите этот параметр. Если данный параметр отключен, то при просмотре записи вместо паролей будут отображаться звездочки. Запись в этом случае не содержит никакой информации о пароле, и увидеть или восстановить пароль по такой записи невозможно.

Внимание: Параметр **Логирование паролей** не действует при вводе пароля на веб-форме. Введенные на веб-формах пароли всегда записываются и отображаются открытым текстом независимо от настройки этого параметра.

Правила

Правила мониторинга активности пользователей определяют условия начала и прекращения записи пользовательской активности. Запись активности начинается при выполнении условий правила, настроенного для данного пользователя, и прекращается, когда эти условия перестают выполняться. Различные правила могут быть настроены для разных пользователей или групп пользователей.

Пользователи и группы, для которых настроены правила мониторинга, перечисляются в дереве консоли под узлом **Мониторинг активности пользователей** > **Правила**. Эти пользователи и группы отображаются также на панели сведений, если в дереве консоли выбран узел **Правила**. Для просмотра правил, настроенных для определенного пользователя или группы, выберите этого пользователя или группу под узлом **Правила** в дереве консоли. Список правил появится на панели сведений (см. Управление существующими правилами).

Контекстное меню узла **Правила** предоставляет следующие команды (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Управление** - Открыть диалоговое окно, в котором можно задавать, просматривать и изменять правила оперативного режима (обычный профиль).
- **Управление офлайновыми настройками** - Открыть диалоговое окно, в котором можно задавать, просматривать и изменять правила автономного режима (офлайн-профиль).

  Диалоговое окно управления правилами устроено одинаково для каждой из этих двух команд, но управляет различными наборами правил в зависимости от используемой команды. Описание этого диалогового окна см. в разделе Диалоговое окно управления правилами.

  Правила автономного режима вступают в силу, когда компьютер не подключен к сети предприятия. Если компьютер подключен к сети или правила автономного режима не настроены, применяются правила оперативного режима. О том, как сервис DeviceLock определяет, подключен ли компьютер к сети предприятия, см. в разделе Настройка конфигурации для автономного режима.
- **Загрузить** - Импортировать правила из файла и применить их для оперативного режима. Откроется диалоговое окно для выбора файла, в который были сохранены правила.
- **Загрузить офлайновые настройки** - Импортировать правила из файла и применить их для автономного режима. Откроется диалоговое окно для выбора файла, в который были сохранены правила.
- **Сохранить** - Экспортировать правила оперативного режима в файл. Откроется диалоговое окно для указания файла, в который будут сохранены правила.
- **Сохранить офлайновые настройки** - Экспортировать правила автономного режима в файл. Откроется диалоговое окно для указания файла, в который будут сохранены правила.
- **Сбросить офлайновые настройки** - Удалить все правила автономного режима, в результате чего правила оперативного режима будут применяться как в оперативном режиме, так и в автономном режиме.

Эти команды (за исключением команды **Сбросить офлайновые настройки**) присутствуют также в контекстном меню на каждом пользователе и группе в узле **Правила**. Кроме того, в данном меню содержится команда **Удалить пользователя**, позволяющая удалить выбранного пользователя или группу из узла **Правила**. Для пользователей и групп, удаленных из этого узла, действие правил прекращается.

В консолях DeviceLock Group Policy Manager и DeviceLock Service Settings Editor контекстное меню узла **Правила** содержит также следующие команды:

- **Сбросить** - Устанавливает правила оперативного режима в состояние "не задано". Данная команда используется, чтобы удалить все правила мониторинга активности пользователей из настроек сервиса DeviceLock для обычного профиля.
- **Удалить офлайновые настройки** - Блокирует наследование правил автономного режима и принудительно применяет правила оперативного режима. Данная команда используется, чтобы применить правила мониторинга активности пользователей для обычного профиля как в оперативном, так и в автономном режиме.

Управление правилами мониторинга предполагает:

- Создание правил
- Управление существующими правилами

Создание правил

Для создания правила требуется выполнить следующие действия:

1. Выполнить команду **Управление** или **Управление офлайновыми настройками** из контекстного меню узла **Мониторинг активности пользователей** > **Правила**.

   Данная команда открывает диалоговое окно для добавления или удаления пользователей и групп, а также правил их мониторинга.

2. В появившемся диалоговом окне указать пользователей или группы, к которым применяется правило, и затем добавить и настроить правило. Подробнее см. в разделе Диалоговое окно управления правилами.

   При добавлении правила открывается отдельное диалоговое окно, предназначенное для его настройки.

3. В появившемся диалоговом окне задать условие начала записи и настроить прочие параметры правила. Подробнее см. в разделе Диалоговое окно настройки правила.

Команда **Управление** используется для создания правил оперативного режима. Если нужно создавать правила автономного режима, используйте команду **Управление офлайновыми настройками**. Правила автономного режима действуют, когда компьютер не подключен к сети предприятия; в противном случае действуют правила оперативного режима. О том, как сервис DeviceLock определяет, подключен ли компьютер к сети предприятия, см. в разделе Настройка конфигурации для автономного режима.

Диалоговое окно управления правилами

Диалоговое окно управления правилами появляется по команде **Управление** или **Управление офлайновыми настройками** из контекстного меню узла **Мониторинг активности пользователей** > **Правила** консоли. Данное окно обеспечивает выполнение следующих задач управления правилами:

- Просмотр или изменение списка пользователей и групп, к которым применяются правила мониторинга.

  Список пользователей и групп приводится в левой части диалогового окна. Для каждого пользователя или группы из этого списка можно настроить одно или несколько правил.

  Под списком находятся кнопки управления:

  - **Добавить** - Открывает стандартное диалоговое окно, предоставляемое операционной системой для выбора пользователей и групп. В список добавляются пользователи и группы, выбранные в этом диалоговом окне.
  - **Удалить** - Удаляет выбранные элементы списка. Для пользователей и групп, удаленных из списка, действие правил прекращается.

- Просмотр, настройка, изменение или удаление правил для определенного пользователя или группы.

  Выберите пользователя или группу в списке слева, чтобы просмотреть правила для этого пользователя или группы. Список правил отображается в правой части диалогового окна. По каждому правилу в списке приводятся следующие сведения:

  - **Имя** - Указывает имя правила.
  - **Запись экрана** - Если этот флажок установлен, то, согласно данному правилу, сервис DeviceLock выполняет видеозапись экрана компьютера пользователя. В противном случае видеозапись не выполняется.
  - **Запись клавиатуры** - Если этот флажок установлен, то, согласно данному правилу, сервис DeviceLock записывает последовательность нажатий клавиш на клавиатуре компьютера пользователя. В противном случае нажатия клавиш не записываются.

  Для каждого правила можно устанавливать или снимать флажки непосредственно в списке правил.

  Под списком находятся кнопки управления:

  - **Добавить** - Открывает диалоговое окно для настройки нового правила.
  - **Редактировать** - Открывает диалоговое окно для просмотра или изменения правила, выбранного в списке.

    Добавление и редактирование правил выполняется с помощью диалогового окна, описанного в разделе Диалоговое окно настройки правила.
  - **Удалить** - Удаляет правило или правила, выбранные в списке. Можно выбрать сразу несколько правил для удаления.

    > **Примечание:** Удаление правила обычно не прерывает запись, начатую этим правилом и продолжающуюся в момент удаления правила. В таком случае действие правила прекращается после завершения записи. Однако если пользователю назначено только одно правило, его удаление приводит к прерыванию записи.

- Экспорт или импорт правил из файла.

  Список пользователей и групп вместе с их правилами можно экспортировать в текстовый файл. Нажмите кнопку **Сохранить**, а затем в появившемся диалоговом окне укажите местоположение и имя файла для хранения данных экспорта.

  Файл экспорта можно импортировать на другой компьютер или использовать в качестве резервной копии правил. Чтобы импортировать пользователей, группы и их правила из файла, нажмите кнопку **Загрузить** и откройте файл в появившемся диалоговом окне.

Диалоговое окно настройки правила

Диалоговое окно настройки правила появляется по нажатию на кнопку **Добавить** или **Редактировать** в диалоговом окне управления правилами и предоставляет возможность задать, просмотреть или изменить следующие параметры правила:

- **Имя** - Присваивается при создании правила и может быть изменено при редактировании правила.
- **Описание** - Любая дополнительная информация о правиле (например, предполагаемое назначение правила).

- **Записывать** - Сервис DeviceLock записывает только выбранные проявления активности пользователя:
  - **Экран** - Если этот флажок установлен, производится видеозапись экрана компьютера пользователя.
  - **Ввод с клавиатуры** - Если этот флажок установлен, записываются нажатия клавиш на клавиатуре компьютера пользователя.
- **Начинать запись, когда выполняется следующее условие** - Запись активности пользователя начинается в зависимости от условия, указанного в правиле. Условие представляет собой логическое выражение, состоящее из одного или нескольких критериев запуска, объединенных логическими операторами. Каждый критерий может принимать логическое значение `true` или `false`. Значение условия вычисляется из текущих значений его критериев, и сервис DeviceLock начинает запись активности пользователя при значении условия равном `true`.

  Некоторые критерии из условия начала записи используются также для определения момента остановки записи. Подробнее об этом см. в разделе Способы прекращения записи.

  В диалоговом окне предоставляется конструктор условий, позволяющий добавлять, изменять или удалять критерии запуска, объединять их по И/ИЛИ и группировать с помощью скобок:

  - Используйте кнопки над списком критериев для добавления или удаления критериев и для изменения порядка их следования в списке:
    - **Добавить** - Добавляет новый критерий в конец списка. Чтобы добавить критерий, нажмите кнопку или дважды щелкните пустую область в списке.
    - **Вставить** - Добавляет новый критерий перед выбранным в списке.

      При добавлении критерия вначале выбирается его тип, а затем выполняется настройка параметров критерия в зависимости от выбранного типа. Подробнее см. в разделе Настройка критериев запуска.
    - **Редактировать** - Позволяет изменить настройку критерия, выбранного в списке, или заменить его другим критерием. Чтобы редактировать критерий, нажмите кнопку или дважды щелкните критерий в списке.

      Для редактировании используется диалоговое окно, в котором можно можно просмотреть/изменить значение параметров данного критерия или выбрать другой критерий на замену критерия в списке. Подробнее см. в разделе Настройка критериев запуска.
    - **Удалить** - Удаляет выбранный критерий из списка. При этом удаляются также логические операторы и скобки, указанные вместе с этим критерием в списке.
    - **^**, **v** (стрелки вверх и вниз) - Перемещают выбранный критерий вверх или вниз по списку.

      Перемещение критериев вверх/вниз по списку может нарушить логическую структуру выражения. Нажмите кнопку **Проверить**, чтобы выполнить ее проверку и отобразить полученное выражение в поле **Результат**.
  - Установите флажок в столбце **НЕ**, чтобы изменить логическое значение критерия на противоположное.
  - Щелкните в столбце с заголовком **(** или **)**, чтобы добавить левые или правые скобки.

Скобки используются, чтобы избежать неоднозначности выражений, содержащих несколько критериев запуска. Например, выражение `А И В ИЛИ С` может означать `(А И В) ИЛИ С` либо `А И (В ИЛИ С)`. Используйте скобки, чтобы точно определить порядок вычисления выражений.

> **Примечание:** При перемещении какой-либо записи на место соседней в списке критериев флажок **НЕ** перемещается вместе с записью, только если количество открывающих скобок меньше или равно количеству закрывающих скобок как в перемещаемой записи, так и в записи, на место которой она перемещается. Если открывающих скобок хотя бы в одной из них больше, чем закрывающих, то этот флажок не переходит на соседнюю запись. Такое решение помогает сохранить логическую структуру выражения при изменении порядка записей в списке.

- Щелкните в столбце **И/ИЛИ**, чтобы выбрать требуемый оператор для объединения критериев в логическое выражение. По умолчанию выбран оператор И, так что запись начинается только при выполнении всех заданных критериев запуска. Выберите оператор ИЛИ, если требуется начинать запись при выполнении хотя бы одного из этих критериев.
- **Проверить** - Проверяет логическую структуру выражения, убирает заведомо лишние скобки и отображает полученное выражение в поле **Результат**.
- **Очистить** - Удаляет из условия все критерии запуска, кроме критерия по умолчанию.

> **Примечание:** Условие начала записи всегда содержит критерий по умолчанию `Пользователь вошел в систему`, так что запись стартует только при условии, что пользователь, к которому применяется данное правило, вошел в систему. Таким образом обеспечивается запись действий вошедшего в систему пользователя в соответствии с текущими правилами мониторинга пользовательской активности.

- **Принудительно прекращать запись через** <число> **сек.** - Если установлен этот флажок, запись начинается при выполнении условия начала записи, а затем прекращается по истечении указанного количества секунд. Если условие начала записи все еще выполняется, запись начинается снова, если только не установлен следующий флажок:
  - **Не запускать правило снова, пока его условие не изменится** - Если этот флажок установлен, запись не возобновляется после принудительного прекращения по времени, даже если условие начала записи все еще выполняется. В этом случае запись возобновится только после того, как это условие перестанет выполняться, а затем снова будет выполнено. Чтобы лучше понять это поведение, предположим, что запись начинается, когда в операционной системе запущен определенный процесс, а затем через некоторое время запись принудительно прекращается. Для возобновления записи в таком случае необходимо остановить данный процесс и запустить его снова.

  Подробнее об этих двух параметрах см. в разделе Способы прекращения записи.

- **Время между снимками экрана:** <число> **сек.** - Определяет частоту снимков экрана в видеозаписи. Сделав снимок экрана, сервис DeviceLock ждет заданное количество секунд, прежде чем сделать следующий снимок, чтобы снизить шансы получения кадров видеозаписи с одинаковым содержимым.

  При создании новых правил по умолчанию используется последнее заданное значение этого параметра. Пусть, например, для некоторого правила было задано значение `3`. После этого значение `3` будет использоваться по умолчанию во всех вновь создаваемых правилах, пока в каком-либо правиле не будет установлено другое значение.

  > **Примечание:** Для использования данного параметра необходимо установить флажок **Записывать** > **Экран**. В противном случае этот параметр недоступен (выделен серым цветом) и не оказывает влияния на запись.

Настройка критериев запуска

При настройке правила мониторинга указывается условие начала записи, состоящее из критериев запуска, объединенных логическими операторами. Каждый критерий запуска соответствует определенному состоянию системы или событию, при котором он выполняется и принимает значение `true` (подробнее см. в разделе Критерии состояния системы и критерии события). Значение условия вычисляется из текущих значений его критериев, и запись может начаться только при значении условия равном `true`.

Входящие в условие начала записи критерии состояния системы используются также для управления остановкой записи. Подробнее об этом см. в разделе Способы прекращения записи.

В правиле можно задать один или несколько критериев запуска, что позволяет начинать запись в различных ситуациях, например, при подключении устройств, запуске приложений или при срабатывании различных политик DeviceLock. Список заданных в правиле критериев запуска отображается в диалоговом окне, в котором можно добавлять, редактировать или удалять критерии из правила (см. Диалоговое окно настройки правила).

Диалоговое окно настройки критериев запуска используется в следующих случаях:

- При добавлении критериев для данного правила можно выбрать нужный критерий из раскрывающегося списка. Затем, в зависимости от того, какой критерий выбран, в диалоговом окне появляется поле параметра для выбранного критерия.
- При редактировании критериев, указанных в правиле, в диалоговом окне отображается выбранный критерий и текущее значение его параметра. Можно просмотреть/изменить значение параметра или выбрать другой критерий взамен текущего.

Ниже приводится краткое описание критериев запуска и их параметров.

- **Пользователь вошел в систему** - Контролируемый пользователь вошел на компьютер или удаленно вошел в систему с помощью служб терминалов или удаленного рабочего стола, успешно пройдя проверку подлинности.

  Примечание: Данный критерий по умолчанию содержится в каждом условии и не может быть удален, поэтому его нет в списке для выбора критериев.

- **Ethernet-подключение существует** - К компьютеру подключен сетевой кабель.
- **VPN-подключение существует** - Компьютер подключен к виртуальной частной сети (VPN).
- **Беспроводное подключение существует** - Компьютер подключен к беспроводной сети по Wi-Fi.
- **IP-адрес назначен** - Сетевой интерфейс компьютера получил IP-адрес.
- **IP-адрес освобожден** - Сетевой интерфейс компьютера освободил свой IP-адрес.
- **Процесс "<имя>" существует** - На компьютере выполняется указанный процесс, запущенный контролируемым пользователем.

  Настраиваемый параметр - путь и имя исполняемого файла процесса (например, `c:\mypath\process.exe`). В параметре можно использовать знаки подстановки: звездочку (*) вместо произвольной последовательности символов, вопросительный знак (?) вместо любого одиночного символа.

  Полезный совет: Если необходимо, чтобы критерий срабатывал независимо от пути к исполняемому файлу, указывайте имя файла следующим образом: `*\<имя файла>`. Пример: `*\excel.exe`

- **Окно "<заголовок>" существует** - В системе существует окно с указанным заголовком, открытое контролируемым пользователем.

  Настраиваемый параметр - заголовок окна. В параметре можно использовать знаки подстановки: звездочку (*) вместо произвольной последовательности символов, вопросительный знак (?) вместо любого одиночного символа.

- **Окно "**<заголовок>**" находится в фокусе** - Окно с указанным заголовком, открытое контролируемым пользователем, активно и может получать ввод с клавиатуры и мыши.

  Настраиваемый параметр - заголовок окна. В параметре можно использовать знаки подстановки: звездочку (*) вместо произвольной последовательности символов, вопросительный знак (?) вместо любого одиночного символа.

- **Сработало контентно-зависимое правило "**<имя>**"** - Контролируемый пользователь попытался отправить или получить данные, соответствующие контентно-зависимому правилу с указанным именем.

  Настраиваемый параметр - имя правила. В параметре можно использовать знаки подстановки: звездочку (*) вместо произвольной последовательности символов, вопросительный знак (?) вместо любого одиночного символа.

  Примечание: Данный критерий относится только к контентно-зависимым правилам управления доступом или правилам обнаружения. Он не реагирует на контентно-зависимые правила теневого копирования.

- **Сработало правило белого списка протоколов "**<имя>**"** - Контролируемый пользователь попытался воспользоваться протоколом, который входит в белый список протоколов согласно правилу с указанным именем.

  Настраиваемый параметр - имя правила. В параметре можно использовать знаки подстановки: звездочку (*) вместо произвольной последовательности символов, вопросительный знак (?) вместо любого одиночного символа.

- **Сработало правило белого списка носителей "**<описание>**"** - Контролируемый пользователь попытался получить доступ к входящему в белый список носителю с указанным описанием.

  Настраиваемый параметр - описание носителя. В параметре можно использовать знаки подстановки: звездочку (*) вместо произвольной последовательности символов, вопросительный знак (?) вместо любого одиночного символа.

- **Сработало правило белого списка USB-устройств "**<описание>**"** - Контролируемый пользователь попытался получить доступ к входящему в белый список USB-устройству с указанным описанием.

  Настраиваемый параметр - описание устройства. В параметре можно использовать знаки подстановки: звездочку (*) вместо произвольной последовательности символов, вопросительный знак (?) вместо любого одиночного символа.

- **Устройство хранения данных присоединено** - Контролируемый пользователь подключил к компьютеру устройство одного из следующих типов: Съемные устройства, MTP, iPhone-устройства, Гибкий диск, Оптический привод, TC-устройства (подключенный диск).

- **Устройство, не предназначенное для хранения данных, присоединено** - Контролируемый пользователь подключил к компьютеру устройство, отличное от следующих типов: Съемные устройства, MTP, iPhone-устройства, Гибкий диск, Оптический привод, TC-устройства (подключенный диск).

  Внимание: Данный критерий не запускает запись активности пользователя при подключении USB HID-устройств (клавиатуры, мыши и т.п.).

- **Компьютер простаивает** <число> **сек.** - Компьютер не заблокирован и на нем нет активности контролируемого пользователя в течение указанного времени.

  В параметре указывается количество секунд бездействия пользователя, после которого данный критерий считается выполненным. Значение параметра должно составлять 3 или более секунд.

  Примечание: Параметр Приостановить запись при неактивности не действует на правила, содержащие данный критерий в условии начала записи. Такие правила не приостанавливают запись по истечении времени, заданного этим параметром.

- **Доступ на чтение к "**<имена>**" запрещен** - DeviceLock заблокировал попытку контролируемого пользователя получить данные из-за отказа в доступе к одному из указанных устройств/протоколов или в соответствии с одной из указанных настроек безопасности.

  В параметре указываются имена устройств, протоколов и/или настроек безопасности. Требуемые имена можно выбрать из выпадающего списка.

- **Доступ на запись к "**<имена>**" запрещен** - DeviceLock заблокировал попытку контролируемого пользователя отправить данные из-за отказа в доступе к одному из указанных устройств/протоколов.

  В параметре указываются имена устройств и/или протоколов. Требуемые имена можно выбрать из выпадающего списка.

Подробнее о некоторых критериях запуска

Значение критерия `Устройство хранения данных присоединено` равно `true` до тех пор, пока к компьютеру присоединено хотя бы одно устройство любого из следующих типов:

- Съемное устройство - Например, подключена USB-флешка.
- MTP - Например, подключен USB-медиаплеер.
- iPhone-устройства - Подключен iPhone или iPad.
- Оптический привод - В дисковод вставлен оптический диск.
- Гибкий диск - В дисковод вставлена дискета.
- TC-устройства (подключенный диск) - Жесткий/съемный/оптический диск подключен в сеансе удаленного рабочего стола или приложения на сервере виртуализации (Remote Desktop Server, Citrix XenDesktop/XenApp и т.п.).

Критерий `Устройство хранения данных присоединено` принимает значение `false`, если к компьютеру не присоединено ни одного устройства какого-либо из перечисленных выше типов.

В случае доступа к устройствам критерий `Доступ на чтение к "<имена>" запрещен` принимает значение `true`, при попытке выполнить какое-либо из следующих запрещенных действий:

- Действия, для запрета которых используются "основные" права доступа Чтение, Чтение с подключенного диска, Доступ к последовательному порту, Доступ к USB-устройствам, Буфер обмена входящий текст / входящие изображения / входящие аудио данные / входящие файлы / входящие неизвестные данные (см. Группа прав "Основные").
- Действия, для запрета которых используется "зашифрованное" право доступа Чтение (см. Группа прав "Зашифрованные").
- Действия, для запрета которых используются "специальные разрешения" Чтение календаря / контакта / электронной почты / вложения / избранного / файла / медиа-данных / бэкапа / заметки / БД Pocket Access / задачи / расхода / документа / неидентифицированного содержимого (см. Группа прав "Специальные разрешения").

В случае доступа к протоколам критерий `Доступ на чтение к "<имена>" запрещен` принимает значение `true` при попытке выполнить какое-либо из следующих запрещенных действий:

- Действия, для запрета которых используются права доступа Отправка/получение данных, Отправка/получение данных (веб), Поиск, Входящие файлы, Входящие звонки (см. Права доступа для протоколов).
- Действия, запрещенные в соответствии с настройками безопасности (при условии, что в параметре критерия установлены соответствующие флажки):
  - Блокировать нераспознанный исходящий SSL-трафик - В параметре критерия необходимо установить флажок `SSL`.
  - Блокировать URL, содержащие IP-адреса - В параметре критерия необходимо установить флажки `IP (TCP)` и/или `IP (UDP)` в зависимости от того, на какие транспортные протоколы (TCP / UDP) должен реагировать данный критерий.
  - Блокировать прокси трафик - В параметре критерия необходимо установить флажки `Proxy (HTTP)`, `Proxy (SOCKS4)` и/или `Proxy (SOCKS5)` в зависимости от того, на прокси-серверы каких типов (HTTP / SOCKS4 / SOCKS5) должен реагировать данный критерий.
  - Блокировать трафик Tor-браузера - В параметре критерия необходимо установить флажок `Tor-браузер`.

  О настройках безопасности см. в разделе Описание настроек безопасности.

В случае доступа к устройствам критерий `Доступ на запись к "<имена>" запрещен` принимает значение `true` при попытке выполнить какое-либо из следующих запрещенных действий:

- Действия, для запрета которых используются "основные" права доступа Запись, Форматирование, Печать, Копирование в буфер обмена, Запись на подключенный диск, Буфер обмена исходящий текст / исходящие изображения / исходящие аудио данные / исходящие файлы / исходящие неизвестные данные (см. Группа прав "Основные").
- Действия, для запрета которых используются "зашифрованные" права доступа Запись, Форматирование (см. Группа прав "Зашифрованные").
- Действия, для запрета которых используются "специальные разрешения" Запись календаря / контакта / электронной почты / вложения / избранного / файла / медиа-данных / бэкапа / заметки / БД Pocket Access / задачи / расхода / документа / неидентифицированного содержимого, Копирование текста / изображения / аудио данных / файла / неидентифицированного содержимого / экрана (см. Группа прав "Специальные разрешения").

Критерий `Доступ на запись к "<имена>" запрещен` не действует при запрете доступа к следующим устройствам: Blackberry-устройства, Bluetooth, ИК-порт, Параллельный порт, Последовательный порт, TC-устройства в случае запрета на Доступ к последовательному порту или запрета на Доступ к USB-устройствам, а также WiFi. Для старта записи по запрету доступа к этим устройствам можно использовать критерий `Доступ на чтение к "<имена>" запрещен`.

В случае доступа к протоколам критерий `Доступ на запись к "<имена>" запрещен` принимает значение `true` при попытке выполнить какое-либо из действий, для запрета которых используются права доступа Исходящие сообщения, Исходящие файлы, POST-запросы, Исходящие звонки (см. Права доступа для протоколов).

Критерии состояния системы и критерии события

Существует два типа критериев запуска: критерии состояния системы - управляются текущим состоянием системы; и критерии события, которые управляются определенными событиями, происходящими в системе.

Критерии состояния системы сохраняют значение `true` до тех пор, пока в системе существуют некоторые объекты, и переключаются в значение `false` только при исчезновении объекта. Например, критерий `Процесс "<имя>" существует` сохраняет значение `true` во время выполнения указанного процесса. Значение критерия меняется на `false` при завершении процесса и остается таким до тех пор, пока процесс не будет запущен снова. Так ведут себя все критерии запуска, обусловленные существованием определенных системных объектов (в данном примере это выполняемые в системе процессы).

Критерии события принимают значение `true` при возникновении определенных событий в системе и переключаются в значение `false` вскоре после того, как событие произошло. Например, критерий `Доступ на запись к "<имена>" запрещен` принимает значение `true`, когда сервис DeviceLock блокирует попытку передачи данных с использованием указанных устройств / протоколов. Затем через некоторое время значение критерия меняется на `false` и остается таким до тех пор, пока не будет заблокирована новая попытка передачи данных. Так ведут себя все критерии запуска, которые обусловлены определенными событиями в системе.

Примечание: Поскольку критерии события принимают значение `true` на очень короткое время, значение их комбинации по И всегда будет `false`. Поэтому нет смысла объединять критерии события по И.

Следующие критерии являются критериями состояния системы:

- Пользователь вошел в систему - `true` все время, пока пользователь не выйдет из системы.
- Ethernet-подключение существует - `true` все время, пока существует данное подключение.
- VPN-подключение существует - `true` все время, пока существует данное подключение.
- Беспроводное подключение существует - `true` все время, пока существует данное подключение.
- Окно "`<заголовок>`" существует - `true` все время, пока существует данное окно.
- Окно "`<заголовок>`" находится в фокусе - `true` все время, пока фокус ввода не уйдет из данного окна.
- Процесс "`<имя>`" существует - `true` все время, пока существует данный процесс.
- Устройство хранения данных присоединено - `true` все время, пока данное устройство подключено.
- Устройство, не предназначенное для хранения данных, присоединено - `true` все время, пока данное устройство подключено.
- Компьютер простаивает `<число>` сек. - `true` все время после срабатывания, пока пользователь не нажимает клавиши на клавиатуре и не двигает / не нажимает мышь.

Следующие критерии являются критериями события:

- IP-адрес назначен - `true` на короткое время после назначения адреса.
- IP-адрес освобожден - `true` на короткое время после освобождения адреса.
- Сработало контентно-зависимое правило "`<имя>`" - `true` на короткое время после срабатывания данного правила.
- Сработало правило белого списка протоколов "`<имя>`" - `true` на короткое время после срабатывания данного правила.
- Сработало правило белого списка носителей "`<описание>`" - `true` на короткое время после срабатывания данного правила.

- Сработало правило белого списка USB-устройств “<описание>” - true на короткое время после срабатывания данного правила.
- Доступ на чтение к “<имена>” запрещен - true на короткое время после запрета чтения.
- Доступ на запись к “<имена>” запрещен - true на короткое время после запрета записи.

Способы прекращения записи

Правила мониторинга активности пользователей предоставляют следующие способы управления запуском и прекращением записи:

- Условие начала записи, согласно которому сервис DeviceLock может начать запись только при значении условия равном true.

  Часть условия начала записи, состоящая только из критериев состояния системы, используется также для управления прекращением записи. Если это так называемое *условие выполнения записи* принимает значение false, запись прекращается.

  Рассмотрим, например, следующее условие начала записи:

  Окно “<заголовок>” существует И Сработало контентно-зависимое правило “<имя>”

  Условием выполнения записи в данном случае будет Окно “<заголовок>” существует. Критерий Сработало контентно-зависимое правило “<имя>” отбрасывается, т.к. это критерий события, а не состояния системы. Подробнее о двух типах критериев запуска см. в разделе Критерии состояния системы и критерии события.

  Подробнее об условии выполнения записи см. в разделе Как вычисляется условие выполнения записи.

- Параметр **Принудительно прекращать запись**, согласно которому сервис DeviceLock прекращает запись по истечении заданного времени, независимо от условия выполнения записи.
- Параметр **Не запускать правило снова, пока его условие не изменится**, согласно которому сервис DeviceLock повторно не запускает запись, прекращенную по истечении заданного времени, пока значение условия начала записи не изменится на false, а затем обратно на true.

Сервис DeviceLock прекращает запись активности пользователя, если:

- Значение условия выполнения записи изменилось на `false`.

  - ИЛИ -

- Истекло время, заданное параметром **Принудительно прекращать запись**.

Это приводит к следующим особенностям правил мониторинга активности пользователей:

- Если не установлен флажок **Принудительно прекращать запись**, запись будет продолжаться до тех пор, пока значение условия выполнения записи равно `true`. Пусть, например, в условии начала записи содержится только критерий `Пользователь вошел в систему`, и не установлен флажок **Принудительно прекращать запись**. В таком случае запись будет выполняться до тех пор, пока пользователь не выйдет из системы.
- Если условие начала записи содержит только критерии события в дополнение к критерию по умолчанию, и не установлен флажок **Принудительно прекращать запись**, запись начнется при возникновении указанных событий и продолжится вплоть до выхода пользователя из системы. В этом случае, чтобы запись прекратилась через определенное время, необходимо установить флажок **Принудительно прекращать запись**.
- Если флажок **Принудительно прекращать запись** установлен, запись прекращается по истечении времени, заданного этим параметром, даже если значение условия выполнения записи равно `true`. В этом случае правило с заданным по умолчанию условием начала записи прекратит запись через указанное время, а затем снова начнет запись, пока пользователь остается в системе. Чтобы запись не запускалась повторно, необходимо установить флажок **Не запускать правило снова, пока его условие не изменится**. Если этот флажок установлен, запись не будет запущена повторно, пока пользователь не выйдет из системы, а затем снова не войдет в систему.

Как вычисляется условие выполнения записи

Условие выполнения записи управляет завершением сеанса записи. Запись заканчивается, когда значение этого условия становится равным `false`. В начале сеанса это значение совпадает со значением условия начала записи. Во время сеанса это значение выражения, представляющего условие начала записи, в котором значения критериев события зафиксированы на момент начала записи. Условие выполнения записи вычисляется путем подстановки в это выражение текущих значений критериев состояния системы, содержащихся в условии начала записи.

Формально значение условия выполнения записи рассчитывается следующим образом. Обозначим логическое выражение условия начала записи через *F(e, s)*, где *e* и *s* - это текущие значения критериев события и критериев состояния системы соответственно. Тогда текущим значением условия выполнения записи является значение логического выражения *F(e0, s)*, где *e0* - это значение критериев события на момент начала сеанса записи.

Примеры правил мониторинга активности пользователей

Приведенные ниже примеры показывают, как работает мониторинг активности пользователей в некоторых типичных сценариях его использования. Эти примеры помогают лучше понять поведение критериев запуска, их роль в условиях начала записи и взаимосвязь с другими параметрами мониторинга, а также условия, приводящие к прекращению записи.

Пример 1: Запись начинается сразу после входа пользователя в систему

Для записи активности пользователя требуется, чтобы пользователь вошел в систему и прошел аутентификацию. Поэтому каждое правило мониторинга пользовательской активности всегда содержит условие начала записи по факту входа пользователя в систему. Таким образом, если задано правило без каких-либо дополнительных критериев запуска, сервис DeviceLock начнет запись сразу после входа пользователя в систему и успешной аутентификации в домене или на локальном ПК.

Чтобы записывать действия пользователя в течение определенного времени после его входа в систему, настройте правило со следующими параметрами:

- `Пользователь вошел в систему` - Заданное по умолчанию условие начала записи.
- `Принудительно прекращать запись через <число> сек.` - Флажок установлен.
- `Не запускать правило снова, пока его условие не изменится` - Флажок установлен.

Так, чтобы запись продолжалась не более часа, необходимо указать значение 3600 секунд:

```
Принудительно прекращать запись через 3600 сек.
```

Согласно данному правилу запись начинается сразу после входа пользователя в систему и прекращается либо через час, либо раньше при выходе пользователя из системы менее чем через час. В следующий раз запись начнется после того, как пользователь выйдет из системы, а затем снова войдет в систему.

Пример 2: Запись использования приложения при подключении VPN

Сервис DeviceLock можно настроить на запись активности пользователя в ситуации, когда работает определенное приложение и установлено подключение виртуальной частной сети (VPN). Соответствующее условие начала записи выглядит следующим образом:

```
Процесс “<имя>” существует И VPN-подключение существует
```

Так, для записи в случае использования Excel должно быть указано имя исполняемого файла `excel.exe`:

```
Процесс “*\excel.exe” существует И VPN-подключение существует
```

Данное объединенное по И условие не вызывает запись, если Excel используется без VPN. Однако после подключения VPN активность пользователя записывается в течение всего времени работы Excel. Запись прекращается при закрытии Excel или при отключении VPN.

Пример 3: Ограниченная по времени запись при подключении по Wi-Fi

Следующий пример - настройка сервиса DeviceLock для записи активности пользователя в течение определенного времени после подключения к беспроводной сети. Настройки правила в этом случае следующие:

- `Беспроводное подключение существует` - Условие начала записи.
- `Принудительно прекращать запись через <число> сек.` - Флажок установлен.
- `Не запускать правило снова, пока его условие не изменится` - Флажок установлен.

Так, чтобы запись продолжалась не более 30 минут после подключения к беспроводной сети, необходимо указать значение 1800 секунд:

```
Принудительно прекращать запись через 1800 сек.
```

Такое правило начинает запись при подключении к беспроводной сети. В данном примере запись длится не более 30 минут и прекращается либо через 30 минут, либо раньше в случае отключения от беспроводной сети менее чем через 30 минут. Запись начнется снова только после отключения и повторного подключения к беспроводной сети.

Пример 4: Запись начинается при запуске определенного приложения

Рассмотрим правило, которое начнет запись в зависимости от того, запущено ли определенное приложение, то есть, запись начнется, если в системе есть процесс с соответствующим именем или окно с соответствующим заголовком. Вот условие начала записи для такого правила:

- `Процесс “<имя>” существует` - Приложение идентифицируется именем процесса.
- `Окно “<заголовок>” существует` - Приложение идентифицируется заголовком окна.

Если в момент запуска приложения сервис DeviceLock уже работает, он заметит, что указанный процесс или окно появилось в системе, и начнет запись. Однако, некоторые процессы могут быть запущены еще до запуска сервиса DeviceLock, например, когда сервис DeviceLock запускается в системе, которая уже работает в течение некоторого времени. В этом случае сервис DeviceLock ищет в системе процессы и окна, указанные в правилах мониторинга активности пользователей, и начинает запись в соответствии с требованиями этих правил. Таким образом, правила реагируют на наличие процесса или окна в системе, а не на факт его появления.

Пример 5: Запись начинается при бездействии пользователя

В этом примере рассматривается правило, при котором DeviceLock начинает запись, если компьютер не используется в течение определенного времени и не заблокирован. Такое правило сработает, если пользователь некоторое время не нажимал клавиши на клавиатуре, не перемещал мышь и не нажимал на нее. В отличие от параметра Приостановить запись при неактивности это правило запускает, а не приостанавливает запись при отсутствии активности пользователя. Условие начала записи выглядит следующим образом:

```
Компьютер простаивает <число> сек.
```

Так, чтобы запись начиналась спустя 5 минут бездействия пользователя, необходимо указать значение 300 секунд:

```
Компьютер простаивает 300 сек.
```

Если действует такое правило, то запись начинается, когда в течение заданного времени на компьютере нет нажатий клавиш или щелчков/движений мыши, и при этом компьютер не заблокирован. Запись прекращается, когда на компьютере происходит какое-либо действие с использованием клавиатуры или мыши.

Что если правило сработает во время записи?

Предположим, что правило A запустило запись действий некоторого пользователя, и во время этой записи сработало правило B для записи действий того же пользователя. В такой ситуации правило B не запускает новую запись, если оба правила настроены на видеозапись. Подробнее данная ситуация рассматривается в следующей таблице.

Параметры правила A	Параметры правила B	Результат срабатывания правила B
Только запись видео	Только запись видео	Новая запись не запускается. Запущенная правилом A запись продолжается, пока ее следует выполнять согласно правилу A и правилу B, и заканчивается только после того, как оба правила прекращают запись.
Запись видео и клавиатуры	Запись видео и клавиатуры	
Только запись видео	Запись видео и клавиатуры	Продолжается ранее запущенная запись. Информация о нажатии клавиш добавляется в нее согласно правилу B.
Запись видео и клавиатуры	Только запись видео	Продолжается ранее запущенная запись. Информация о нажатии клавиш добавляется в нее согласно правилу A.
Только запись клавиатуры	Запись видео и/или клавиатуры	Правило B запускает новую запись. Правило A продолжает свою запись.
Запись видео и/или клавиатуры	Только запись клавиатуры	

Если во время записи по некоторому правилу A сработало несколько других правил (B, C, . . .), то новая запись не запускается, только если каждое правило A, B, C, . . . записывает видео и, возможно, нажатия клавиш. В противном случае может стартовать новая запись видео и/или клавиатуры. Правила, срабатывающие во время видеозаписи без запуска новой записи, перечисляются в поле **Правило** просмотрщика журнала активности пользователей (см. Список сеансов мониторинга), а также на водяном знаке видеозаписи. Видеозапись продолжается до тех пор, пока ее следует выполнять согласно сработавшим правилам, и заканчивается только после того, как все эти правила прекращают запись. Запись нажатий на клавиши выполняется в соответствии с настройками сработавших правил.

Предположим, что некоторое правило запустило запись действий пользователя, и во время этой записи то же самое правило сработало еще раз для того же пользователя. В таком случае новая запись не начинается, даже если правило записывает только нажатия клавиш. Запись будет продолжена в соответствии с новым срабатыванием правила. Смещение времени нового срабатывания правила отображается в квадратных скобках в поле **Правило** просмотрщика журнала активности пользователей (см. Список сеансов мониторинга).

Что если нечего записывать?

Срабатывание правила не приводит к созданию записи в журнале активности пользователей, если за все время выполнения записи сервис DeviceLock не успел зафиксировать никаких действий пользователя. Подробнее данная ситуация рассматривается в следующей таблице.

Записывается	За время записи
Только экран	Не сделано ни одного снимка экрана.
Только ввод с клавиатуры	Не перехвачено ни одного нажатия клавиш.
Экран и ввод с клавиатуры	Не сделано ни одного снимка экрана и не перехвачено ни одного нажатия клавиш.

Во всех перечисленных случаях запись в журнале активности пользователей не создается.

Управление существующими правилами

Пользователи и группы с настроенными правилами мониторинга активности пользователей перечисляются под узлом **Мониторинг активности пользователей** > **Правила** в дереве консоли, а также на панели сведений, если в дереве консоли выбран узел **Правила**. Для просмотра правил для какого-либо пользователя или группы, выберите этого пользователя или группу в дереве консоли или дважды щелкните пользователя или группу в списке на панели сведений. В результате на панели сведений отображаются правила для данного пользователя или группы со следующей информацией о каждом правиле:

- **Имя** - Отображает имя правила. Имя присваивается при создании правила и может быть изменено при редактировании правила.
- **Описание** - Отображает описание правила. В описании может предоставляться какая-либо дополнительная информация о правиле (например, его предназначение). Описание можно задать или изменить при создании или редактировании правила.
- **Запись экрана** - Указывает, требует ли данное правило выполнять видеозапись экрана компьютера пользователя. Этот параметр можно задать или изменить при создании или редактировании правила.
- **Запись клавиатуры** - Указывает, требует ли данное правило записывать нажатия клавиш на клавиатуре компьютера пользователя. Этот параметр можно задать или изменить при создании или редактировании правила.
- **Условие** - Указывает заданное в правиле условие начала записи. Условие представляет собой логическое выражение, состоящее из одного или нескольких критериев запуска, объединенных логическими операторами. Запись начинается, если данное выражение принимает значение `true`. Условие начала записи можно задать или изменить при создании или редактировании правила.

  Примечание: Поскольку известно, что условие всегда содержит критерий запуска `Пользователь вошел в систему`, этот критерий обычно не отображается в поле **Условие**. Он отображается, только если в условии нет других критериев запуска.

- **Профиль** - Возможные значения:
  - **Обычный** - Правило используется, если компьютер подключен к сети предприятия (правило оперативного режима). Данный профиль присваивается правилам, созданным с помощью команды **Управление**.
  - **Офлайн** - Правило используется, если компьютер отключен от сети предприятия (правило автономного режима). Данный профиль присваивается правилам, созданным с помощью команды **Управление офлайновыми настройками**.

  Профиль присваивается при создании правила и не может быть изменен после того, как правило создано.

  О том, как сервис DeviceLock определяет, подключен ли компьютер к сети предприятия, см. в разделе Настройка конфигурации для автономного режима.

В контекстном меню пользователя или группы содержатся все команды из контекстного меню узла Правила, за исключением команды **Сбросить офлайновые настройки**. В нем также имеется команда **Удалить пользователя**, позволяющая удалить выбранного пользователя или группу из узла **Правила**. Для пользователей и групп, удаленных из этого узла, действие правил прекращается.

Контекстное меню правила в списке на панели сведений предоставляет следующие команды:

- **Управление** - Открыть диалоговое окно, в котором можно задавать, просматривать и изменять правила мониторинга активности пользователей. В случае выбора команды на правиле обычного профиля открывается окно для управления правилами оперативного режима. В случае выбора команды на правиле офлайн-профиля открывается окно для управления правилами автономного режима. Окно устроено одинаково в каждом из этих двух случаев, но служит для управления различными наборами правил в зависимости от профиля того правила, на котором выбрана команда **Управление**. Описание этого окна см. в разделе Диалоговое окно управления правилами.
- **Редактировать** - Открыть диалоговое окно для просмотра или изменения правила, выбранного в списке. Описание этого диалогового окна см. в разделе Диалоговое окно настройки правила.
- **Запись экрана** - Переключить параметр правила, управляющий видеозаписью экрана компьютера пользователя. Щелкните эту команду, чтобы разрешить или запретить видеозапись. Если выбрано несколько правил, то вместо этой команды отображаются команды **Включить запись экрана** / **Выключить запись экрана**.
- **Запись клавиатуры** - Переключить параметр правила, управляющий записью нажатий клавиш на клавиатуре компьютера пользователя. Щелкните эту команду, чтобы разрешить или запретить запись нажатий на клавиши. Если выбрано несколько правил, то вместо этой команды отображаются команды **Включить запись клавиатуры** / **Выключить запись клавиатуры**.
- **Удалить** - Удалить правило или правила, выбранные в списке. Можно выбрать сразу несколько правил для удаления.

> **Примечание:** Удаление правила обычно не прерывает запись, начатую этим правилом и продолжающуюся в момент удаления правила. В таком случае действие правила прекращается после завершения записи. Однако если пользователю назначено только одно правило, его удаление приводит к прерыванию записи.

Просмотр активности пользователей

Данные мониторинга активности пользователей первоначально сохраняются на локальном компьютере, что позволяет просматривать локальные записи пользовательских действий при помощи просмотрщика журнала активности пользователей в консоли DeviceLock Management Console, подключенной к сервису DeviceLock. Таким путем можно получить доступ только к записям, которые были выполнены сервисом DeviceLock на локальном компьютере.

Для централизованного просмотра и анализа записей с различных компьютеров необходимо передавать данные мониторинга активности пользователей на сервер DeviceLock Enterprise Server, включив параметр сервиса DeviceLock Отправлять данные теневого копирования на сервер. Серверы для сбора и хранения данных задаются параметром DeviceLock Enterprise Server(ы). Каждый сервер собирает только данные о пользователях и группах, назначенным этому серверу. При необходимости записи активности пользователей можно объединить для просмотра и анализа на центральном сервере (см. Консолидация журналов).

Данные мониторинга активности пользователей хранятся там же, где файлы теневого копирования. Сервис DeviceLock хранит их в папке, заданной параметром Локальная директория. Для сервера DeviceLock Enterprise Server место хранения данных определяется параметром **Путь к хранилищу** (см. Настройки сервера). Подробнее о выборе места хранения см. в описании параметра Хранить файлы теневого копирования в базе данных.

Записи мониторинга активности пользователей можно просматривать на панели сведений консоли DeviceLock Management Console, выбрав в дереве консоли **Просмотрщик журнала активности пользователей**. Для просмотра локальных записей выберите **Сервис DeviceLock** > **Мониторинг активности пользователей** > **Просмотрщик журнала активности пользователей** в консоли, подключенной к сервису DeviceLock. Для просмотра записей, хранящихся на сервере, выберите **DeviceLock Enterprise Server** > **Просмотрщик журнала активности пользователей** в консоли, подключенной к серверу DeviceLock Enterprise Server. Для управления журналом можно использовать команды контекстного меню узла **Просмотрщик журнала активности пользователей** (описание команд см. в разделе Управление журналом активности пользователей).

Панель сведений просмотрщика разделена на верхнюю и нижнюю области. В верхней области отображается список сеансов мониторинга, перечисляющий все имеющиеся в журнале записи активности пользователей. Нижняя область служит для просмотра сеанса мониторинга, позволяя просматривать видеозапись экрана компьютера пользователя вместе с записью ввода с клавиатуры и другими данными.

Внимание:

- Для сбора данных мониторинга активности пользователей на сервере DeviceLock Enterprise Server должна быть установлена основная лицензия DeviceLock. Количество компьютеров, с которых сервер собирает данные мониторинга активности пользователей, не может быть больше указанного в этой лицензии.
- Для применения серверных политик и задач мониторинга компьютеров, в которых заданы параметры и правила мониторинга активности пользователей, на сервере DeviceLock Enterprise Server должна быть установлена лицензия DeviceLock UAM. Количество компьютеров, к которым применяются такие политики и задачи, не может быть больше указанного в этой лицензии.

Инструкции по установке лицензий см. в разделе Активация серверных лицензий.

Список сеансов мониторинга

Для просмотра активности пользователей выберите в дереве консоли **Просмотрщик журнала активности пользователей**. Верхняя часть панели сведений содержит список хранящихся в журнале записей пользовательской активности - сеансов мониторинга. В списке предоставляются следующие сведения по каждой записи:

- **Компьютер** - Имя компьютера, на котором был записан данный сеанс мониторинга.

  Имя компьютера отображается только в журнале сервера DeviceLock Enterprise Server. Эта информация отсутствует в журнале сервиса DeviceLock.

- **Дата/Время** - Дата и время начала записи данного сеанса.
- **Тип** - Виды записи, доступные в данном сеансе. Возможные значения:
  - **Видеозапись** - Только запись экрана компьютера.
  - **Запись клавиатуры** - Только запись нажатий клавиш на клавиатуре компьютера.
  - **Видеозапись, Запись клавиатуры** - Запись экрана и запись нажатий клавиш.

  Примечание: Если в сеансе содержится только запись экрана или только запись нажатий на клавиши, то тип сеанса будет **Видеозапись** или **Запись клавиатуры**, соответственно, даже если правило мониторинга настроено на запись экрана и клавиатуры. Это происходит, например, когда сервис DeviceLock не успевает сделать снимки экрана или перехватить нажатия клавиш во время записи.

- **Правило** - Имя правила, вызвавшего запись. Здесь могут быть перечислены несколько правил, если во время данной записи сработало более одного правила.
- **Причина** - Критерии запуска правила, которое вызвало запись. В случае нескольких правил для каждого из них отдельно перечисляются его критерии запуска.

  Примечание: Поскольку известно, что правило всегда имеет критерий запуска `Пользователь вошел в систему`, этот критерий обычно не отображается в поле **Причина**. Он отображается, только если у правила нет других критериев запуска.

- **Продолжительность** - Промежуток времени (часы, минуты и секунды), в течение которого выполнялась запись.
- **Пользователь** - Имя пользователя, активность которого записана в данном сеансе.
- **Дата/Время сбора** - Дата и время, когда сервер DeviceLock Enterprise Server получил данную запись от сервиса DeviceLock.

  Дата и время получения записи отображается только в журнале сервера DeviceLock Enterprise Server. Эта информация отсутствует в журнале сервиса DeviceLock.

- **Сервер** - Имя компьютера, на котором работает сервер DeviceLock Enterprise Server, получивший данную запись от сервиса DeviceLock.

  Имя компьютера отображается только в журнале сервера DeviceLock Enterprise Server. Эта информация отсутствует в журнале сервиса DeviceLock.

- **Сервер консолидации** - Имя удаленного сервера, с которого данная запись была последний раз получена при консолидации журналов (см. Консолидация журналов).
- **Дата/Время консолидации** - Дата и время, когда запись была последний раз получена с удаленного сервера при консолидации журналов (см. Консолидация журналов).

  Сервер и дата/время консолидации отображаются только в журнале сервера DeviceLock Enterprise Server. Эта информация отсутствует в журнале сервиса DeviceLock.

В контекстном меню каждой записи на панели сведений предоставляются следующие команды управления записью (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Открыть** - Открыть записанный файл в приложении, которое зарегистрировано для файлов данного типа в операционной системе. Если сеанс содержит запись экрана, то открывается записанный видео файл. Если сеанс содержит только запись клавиатуры, открывается файл, в котором записаны нажатия клавиш.
- **Сохранить** - Сохранить записанное видео и/или запись ввода с клавиатуры в указанный файл. Запись клавиатуры (при ее наличии) сохраняется в виде HTML-файла.
- **Удалить** - Удалить выбранную запись. Используя клавиши Ctrl и Shift, можно выбрать и удалить несколько записей одновременно.

В контекстном меню каждой записи присутствуют также команды управления журналом, описанные в разделе Управление журналом активности пользователей.

Для поиска интересующих сеансов используйте фильтрацию (см. Фильтрация списка сеансов). Выберите сеанс в списке, чтобы просмотреть его запись (см. Просмотр сеанса мониторинга).

Фильтрация списка сеансов

Если в дереве консоли выбран узел **Просмотрщик журнала активности пользователей**, на панели сведений отображается список всех доступных сеансов мониторинга. Для поиска определенных сеансов в этом списке можно использовать следующие средства:

- Команда **Быстрые фильтры** оставляет в списке только сеансы за определенный период (день, неделя, месяц, год). Подробнее см. в разделе Управление журналом активности пользователей.
- Команда **Фильтр** сужает список в соответствии с указанными условиями (дата записи, имя пользователя, записанные данные и т.п.). Подробнее см. в разделе Фильтр журнала активности пользователей.

Просмотр сеанса мониторинга

Если в дереве консоли выбрать узел **DeviceLock Enterprise Server** > **Просмотрщик журнала активности пользователей**, а затем выбрать какой-либо сеанс мониторинга из списка на панели сведений, в нижней части панели сведений можно просматривать:

- Видеозапись экрана - Видеоплеер позволяет просматривать видеозапись экрана пользовательского компьютера, если такая запись выполнялась согласно правилам данного сеанса.
- Запись клавиатуры - В таблице отображаются записи нажатий клавиш на клавиатуре пользовательского компьютера, если нажатия на клавиши записывались в соответствии с правилами данного сеанса.
- Список процессов - В отдельной таблице перечисляются все процессы, запущенные во время данного сеанса пользователем, за которым ведется наблюдение.

Чтобы начать просмотр сеанса мониторинга, дважды щелкните этот сеанс в списке на панели сведений. Для управления сеансами используйте команды из контекстного меню, описанные в разделе Список сеансов мониторинга.

Просмотр видеозаписи экрана

Для воспроизведения записи экрана компьютера используется видеоплеер в нижней части панели сведений. Чтобы начать воспроизведение, выберите требуемый сеанс мониторинга в списке на панели сведений и щелкните внутри видеоплеера, или дважды щелкните этот сеанс мониторинга в списке.

В нижней части плеера расположены следующие элементы управления просмотром видео:

- Кнопка управления воспроизведением - Расположена в левом нижнем углу. Нажимайте эту кнопку, чтобы начать / приостановить / возобновить воспроизведение.
- Индикатор воспроизведения - Панель над кнопкой управления позволяет:
  - Следить за ходом воспроизведения. Движущийся ползунок на полосе индикатора указывает текущую позицию во времени воспроизведения записи.
  - Просматривать временную шкалу воспроизведения. Наведите указатель мыши на ползунок или на полосу индикатора, чтобы отобразить время в минутах и секундах от начала записи до соответствующей позиции на индикаторе.
  - Начать воспроизведение с определенного момента записи. Перетащите ползунок или щелкните на полосе индикатора, чтобы перейти к желаемой позиции во времени воспроизведения записи.
- Текущее время воспроизведения / общая продолжительность видео - Отображается рядом с кнопкой управления в формате `мин:сек / мин:сек`.
- Кнопка полноэкранного режима - Расположена в правом нижнем углу. Нажмите эту кнопку, чтобы развернуть видео на весь экран. Для выхода из полноэкранного режима нажмите клавишу `Esc`.

Для прокрутки видеозаписи при воспроизведении можно использовать клавиши со стрелками. Нажмите клавишу “стрелка влево”, чтобы вернуться на 10 секунд назад; нажмите клавишу “стрелка вправо”, чтобы перейти на 10 секунд вперед. Для непрерывной перемотки назад или вперед удерживайте нажатой клавишу “стрелка влево” или “стрелка вправо” соответственно.

У плеера может быть несколько вкладок при наличии нескольких дисплеев на компьютере пользователя. Каждая вкладка воспроизводит запись экрана определенного дисплея, если для каждого из них предусмотрена отдельная видеозапись в соответствии с настройкой Несколько дисплеев.

Просмотр записи клавиатуры

Таблица в нижней части панели сведений служит для просмотра записи нажатий клавиш на клавиатуре. По каждой записи нажатий в таблице предоставляется следующая информация:

- **Дата/Время** - Дата и время начала ввода с клавиатуры.
- **Заголовок окна** - Заголовок окна приложения, в котором выполнялся ввод с клавиатуры.
- **Ввод с клавиатуры** - Введенные пользователем печатные символы, а также возможно имена нажатых не символьных клавиш в квадратных скобках.
- **Имя процесса** - Имя и путь к исполняемому файлу процесса (приложения), в котором выполнялся ввод с клавиатуры. Идентификатор данного процесса (PID) отображается в скобках после имени файла.

По умолчанию в поле **Ввод с клавиатуры** отображаются только печатные символы. Нажатия не символьных клавиш (таких как `Shift`, `Alt`, `Enter`, `Right`, `Left` и т.п.) пропускаются. Для просмотра всех записанных нажатий на клавиши установите флажок **Показать специальные клавиши**. Если этот флажок установлен, отображаются введенные печатные символы, а также имена нажатых не символьных клавиш. Имена таких клавиш заключены в квадратные скобки (например, `[Shift]серийный номер`).

Если запись была выполнена с включенным параметром Логирование паролей, введенные пользователем пароли отображаются красным цветом в поле **Ввод с клавиатуры**. Если во время записи этот параметр был отключен, то вместо паролей отображаются звездочки.

Примечание: При вводе в диалоговом окне **Безопасность Windows** имя пользователя и пароль регистрируются совместно. Поэтому в таком случае в поле **Ввод с клавиатуры** имя пользователя также выделяется красным цветом или заменяется звездочками в зависимости от того, был ли во время записи включен параметр Логирование паролей.

На записи клавиатуры предоставляется контекстное меню со следующими командами:

- **Копировать** (Ctrl+C) - Позволяет скопировать выбранный текст записи в буфер обмена.
- **Выбрать все** (Ctrl+A) - Позволяет выбрать весь текст записи клавиатуры.
- **Печать** (Ctrl+P) - Позволяет распечатать запись клавиатуры на принтере.

Список процессов

Во время записи пользовательской активности регистрируются все процессы, запущенные пользователем, за которым ведется наблюдение. При просмотре записи отображается список со следующей информацией по каждому такому процессу:

- **Имя процесса** - Имя исполняемого файла данного процесса. Чтобы увидеть полный путь к файлу, наведите указатель мыши на имя файла.
- **Заголовок окна** - Заголовок окна, открытого данным процессом. Пусто, если окно процесса было скрыто. Для включения таких процессов в список выберите параметр **Показать скрытые процессы**.
- **Дата/Время начала** - Дата и время, когда процесс был запущен.
- **Дата/Время завершения** - Дата и время, когда процесс закончился. Пусто, если процесс не закончился во время сеанса мониторинга.
- **ID процесса** - Числовой идентификатор, который был назначен операционной системой данному процессу во время его выполнения.

Место, где отображается список процессов, зависит от содержимого записи сеанса:

Содержимое сеанса	Место списка процессов
Видеозапись экрана и запись клавиатуры	На вкладке **Процессы** в области просмотра записи клавиатуры.
Только видеозапись экрана	Справа от видеоплеера.
Только запись клавиатуры	Справа от области просмотра записи клавиатуры.

Управление журналом активности пользователей

В контекстном меню узла **Просмотрщик журнала активности пользователей** предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное количество записей в журнале (см. Настройки журнала активности пользователей). Эта команда предоставляется только для журнала на сервере DeviceLock Enterprise Server.

  Команда **Настройки** отсутствует в меню журнала активности пользователей на сервисе DeviceLock. Размер журнала в этом случае зависит от параметра Локальная квота (%). Подробнее см. в разделе Квота локального хранилища данных.

- **Обновить** - Обновить список записей с учетом последних изменений.
- **Фильтр** - Отображать только записи, которые удовлетворяют заданным условиям (см. Фильтр журнала активности пользователей).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра записей за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).

- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Отправить данные на сервер** - Как можно скорее отправить данные журнала на сервер, заданный параметром DeviceLock Enterprise Server(ы). Поскольку сервер DeviceLock Enterprise Server автоматически собирает данные журналов по мере их накопления сервисом DeviceLock, использовать эту команду не обязательно.

  Команда **Отправить данные на сервер** предоставляется только для журнала на сервисе DeviceLock. На сервере DeviceLock Enterprise Server эта команда отсутствует. Передать журнал с одного сервера на другой можно с помощью консолидации журналов.

Эти команды присутствуют также в контекстном меню каждой записи на панели сведений (см. Список сеансов мониторинга).

Квота локального хранилища данных

Журнал активности пользователей на контролируемом компьютере зависит от параметра Локальная квота (%) сервиса DeviceLock на этом компьютере. В случае превышения квоты правила мониторинга активности пользователей перестают срабатывать, и новые записи в журнал не добавляются. В журнале аудита регистрируется событие **Локальная квота исчерпана** со следующим сообщением: "Правила мониторинга активности пользователей отключены из-за недостаточного места в локальном хранилище (`%SHADOW_PATH%`)".

Если квота оказывается превышена во время выполнения записи активности пользователя, запись прекращается, и записанные файлы сохраняются в локальном журнале активности пользователей. Это гарантирует, что завершенная часть записи не будет потеряна.

При превышении квоты мониторинг активности пользователей приостанавливается до тех пор, пока не будет освобождено место в локальном хранилище данных (например, путем отправки журналов на сервер DeviceLock Enterprise Server). Мониторинг возобновляется автоматически, как только в локальном хранилище данных появится достаточно свободного места.

Настройки журнала активности пользователей

Диалоговое окно управления настройками журнала на сервере DeviceLock Enterprise Server позволяет просмотреть или изменить следующие параметры:

- **Контролировать размер журнала** - Установите этот флажок, чтобы контролировать количество записей в журнале и удалять устаревшие записи. Если этот флажок не установлен, для хранения журнала используется все доступное дисковое пространство.
- **Сохранять события за последние** <число> **дней** - Если выбран этот параметр, в журнале хранятся записи не старше заданного количества дней.
- **Максимальный размер:** <число> **записей** - Если выбран этот параметр, в журнале хранится не более заданного количества записей. Для данного параметра необходимо выбрать, какое действие будет выполняться при достижении максимального размера журнала:
    - **Затирать старые события по необходимости** - Новые записи продолжают сохраняться при достижении максимального размера журнала. Каждая новая запись заменяет собой самую старую запись в журнале.
    - **Затирать события старше** <число> **дней** - Новые записи заменяют собой только записи, хранящиеся дольше заданного количества дней. Поддерживаемая настройка - до 32 767 дней.
    - **Не затирать события (очистка журнала вручную)** - При достижении максимального размера журнала новые записи не добавляются. Чтобы обеспечить их добавление, необходимо вручную удалить старые записи.

Чтобы использовать настройки по умолчанию, нажмите кнопку **Восстановить умолчания**. В результате будут установлены следующие настройки:

- Максимальный размер: 10 000 записей
- Затирать события старше 7 дней

Примечание:

- Старые записи удаляются по дате, указанной в столбце **Дата/Время сбора** (если запись была получена непосредственно от сервиса DeviceLock), либо по дате, указанной в столбце **Дата/Время консолидации** (если запись была получена от другого сервера посредством консолидации).
- Если в журнале нет места для новых записей, а настройки журнала не позволяют удалить старые записи, новые записи добавляться в журнал не будут. В этом случае при сборе журналов с других компьютеров те записи, которые не могут быть добавлены в журнал на сервере, остаются на своих компьютерах.

Фильтр журнала активности пользователей

После применения фильтра в консоли отображаются сеансы мониторинга в соответствии с настройками фильтра. Для доступа к настройкам служит команда **Фильтр** из контекстного меню журнала активности пользователей, открывающая диалоговое окно, в котором можно задать, просмотреть или изменить настройки фильтра.

Предусмотрены два типа фильтра:

- **Включить** - Отображать только сеансы, которые соответствуют заданным условиям. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Включить** и задайте условия на этой вкладке.
- **Исключить** - Не отображать сеансы, которые соответствуют заданным условиям. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Исключить** и задайте условия на этой вкладке.

Фильтр можно временно выключить. Для этого снимите флажок **Включить фильтр**.

Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

Когда фильтр включен, можно настроить условия фильтрации, задав необходимые значения в следующих полях:

- **Тип** - Фильтрация по доступным видам записи:
  - **Видеозапись** - Флажок для фильтрации сеансов, содержащих только видеозапись экрана компьютера.
  - **Запись клавиатуры** - Флажок для фильтрации сеансов, содержащих только запись нажатий на клавиши.

  Внимание:
  - Если установлен только флажок **Видеозапись**, фильтру соответствуют только сеансы с видеозаписью без записи нажатий на клавиши.
  - Если установлен только флажок **Запись клавиатуры**, фильтру соответствуют только сеансы с записью нажатий на клавиши, без видеозаписи.
  - Если установлены оба флажка, фильтру соответствуют сеансы с видеозаписью и/или записью нажатий на клавиши.

- **Компьютер** - Имя компьютера, на котором был записан сеанс мониторинга. Можно использовать знаки подстановки, а также указать несколько имен через точку с запятой.

  Поле **Компьютер** имеется только в фильтре журнала на сервере DeviceLock Enterprise Server. В фильтре журнала на сервисе DeviceLock это поле отсутствует.

- **Правило** - Имя правила, вызвавшего запись. Можно использовать знаки подстановки, а также указать несколько правил через точку с запятой.
- **Причина** - Описание причины, по которой сработало правило, вызвавшее запись. Можно использовать знаки подстановки, а также указать несколько причин через точку с запятой.
- **Продолжительность** - Промежуток времени (дни, часы, минуты и секунды), в течение которого выполнялась запись. Возможные варианты настройки: больше, меньше или равно заданному значению, или в промежутке между заданной парой значений.

  Значение вводится в формате `дни:часы:минуты:секунды`. Незначащие нули можно опускать. Например, 00:00:30:00 эквивалентно 30:00 и означает 30 минут.

- **Пользователь** - Имя пользователя, активность которого была записана в сеансе мониторинга. Можно использовать знаки подстановки, а также указать несколько имен через точку с запятой.

- **Сервер** - Имя компьютера, на котором работает сервер DeviceLock Enterprise Server, получивший запись от сервиса DeviceLock. Можно использовать знаки подстановки, а также указать несколько имен через точку с запятой.

  Поле **Сервер** имеется только в фильтре журнала на сервере DeviceLock Enterprise Server. В фильтре журнала на сервисе DeviceLock это поле отсутствует.

- **Запись клавиатуры** - Фильтрация по данным, которые пользователь вводил с клавиатуры во время сеанса мониторинга:

  - **Заголовок окна** - Заголовок окна приложения, в котором выполнялся ввод с клавиатуры. Можно использовать знаки подстановки, а также указать несколько заголовков через точку с запятой.

  - **Ввод с клавиатуры** - Слова/фразы, введенные пользователем с клавиатуры. Можно использовать знаки подстановки, а также указать несколько фраз через точку с запятой.

    Примечание:

    - Фильтрация применяется только к печатным символам. Фильтр не замечает имена нажатых не символьных клавиш, такие как `Shift`, `Alt`, `Del`, `Left`, `Right`, `End` и т.п., которые также регистрируются в записи клавиатуры. Например, строка фильтра `серийный номер` соответствует как записи `серийный номер`, так и записи `серийный [Shift]номер`.
    - Чтобы настроить фильтр, которому соответствуют записи, содержащие пароли, используйте следующую маску в поле **Ввод с клавиатуры**: `*<password>*</password>*`

  - **Имя процесса** - Имя и путь к исполняемому файлу процесса (приложения), в котором выполнялся ввод с клавиатуры. Можно использовать знаки подстановки, а также указать несколько процессов через точку с запятой.

- **С**, **По** - Временной диапазон фильтрации по дате и времени начала записи сеанса. Имеется в фильтре журнала на сервисе DeviceLock.

- **Дата/Время генерации** - Временной диапазон фильтрации записей по дате и времени начала записи сеанса сервисом DeviceLock. Имеется только в фильтре журнала на сервере DeviceLock Enterprise Server.

- **Дата/Время сбора** - Временной диапазон фильтрации записей по дате и времени их получения от сервиса DeviceLock. Имеется только в фильтре журнала на сервере DeviceLock Enterprise Server.

- **Консолидация** - Поля для фильтрации по данным, относящимся к консолидации журналов (см. Консолидация журналов):

  - **Сервер** - Имя удаленного сервера, с которого данная запись была последний раз получена при консолидации журналов. Можно использовать знаки подстановки, а также указать несколько имен через точку с запятой.

  - **С**, **По** - Настройки временного диапазона для фильтрации записей по времени, когда они были последний раз получены с удаленного сервера при консолидации журналов.

  Поля, связанные с консолидацией, имеются только в фильтре журнала на сервере DeviceLock Enterprise Server. Они отсутствуют в фильтре журнала на сервисе DeviceLock.

Для каждого временного диапазона предусмотрены следующие настройки:

- **С** - Начало диапазона. Возможные значения:
  - **Первой записи** - Фильтровать записи, начиная с самой ранней даты и времени в соответствующем поле журнала.
  - **Записи от** - Фильтровать записи, начиная с указанной даты и времени.
- **По** - Конец диапазона. Возможные значения:
  - **Последнюю запись** - Фильтровать записи, заканчивая самой поздней датой и временем в соответствующем поле журнала.
  - **Записи от** - Фильтровать записи, заканчивая указанной датой и временем.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что сеанс соответствует фильтру, если он соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В строковых полях фильтра можно указывать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что сеанс соответствует условию фильтра по данному полю, если он соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

11

Сервер DeviceLock Enterprise Server

В этой главе:

Администрирование сервера DeviceLock Enterprise Server

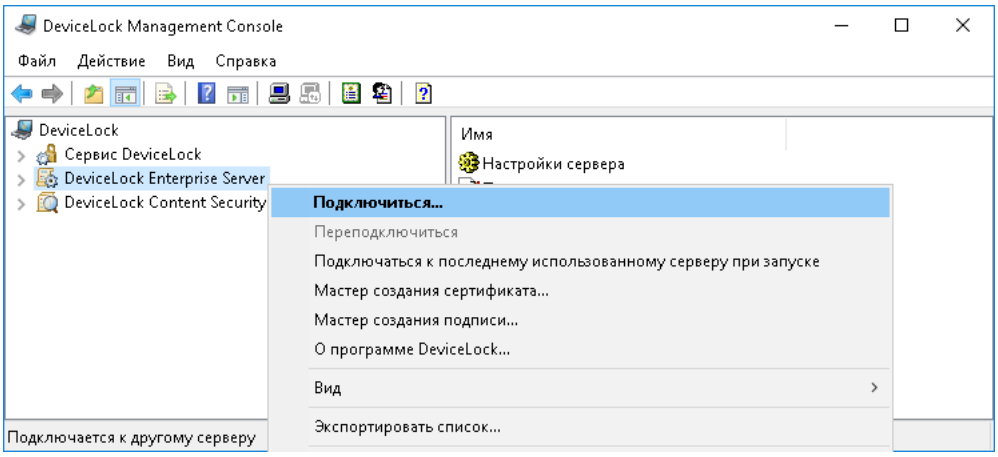
Средства просмотра журналов DeviceLock

Консолидация журналов

Мониторинг

Администрирование сервера DeviceLock Enterprise Server

Раскройте узел **DeviceLock Enterprise Server** в дереве консоли, чтобы получить доступ к функциям и настройкам данного сервера.



По нажатию правой кнопки мыши на узле **DeviceLock Enterprise Server** появляется контекстное меню:

- **Подключиться** - Для подключения консоли к удаленному или локальному компьютеру. Подробнее см. в разделе Подключение к компьютеру данного руководства.

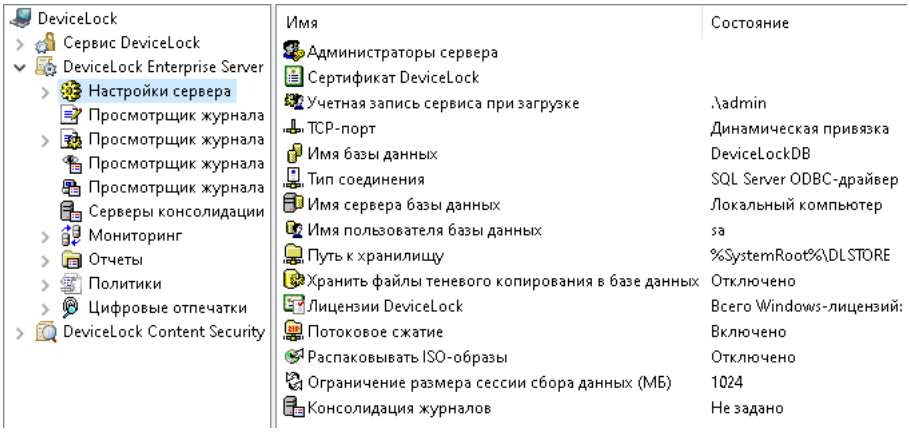
  При подключении к компьютеру, на котором установлена предыдущая версия DeviceLock Enterprise Server, появляется следующее сообщение: “Версии продукта на машинах клиента и сервера не совпадают.” В этом случае необходимо установить новую версию DeviceLock Enterprise Server на этот компьютер. Информацию относительно установки сервера вы можете найти в разделе Установка DeviceLock Enterprise Server данного руководства.

- **Переподключиться** - Повторно подключается к тому же компьютеру.

- **Подключаться к последнему использованному серверу при запуске** - Установите этот флажок для того, чтобы при каждом запуске консоль управления автоматически подключалась к серверу, который использовался в предыдущий раз.
- **Мастер создания сертификата** - Запускает программу для создания сертификатов DeviceLock. Подробнее см. в разделе Создание сертификата.
- **Мастер создания подписи** - Запускает программу для авторизации устройств во временном белом списке и подписывания файлов с настройками сервиса DeviceLock. Подробнее см. в разделе Мастер создания подписи.
- **О программе DeviceLock** - Отображает диалоговое окно с информацией о версии и установленных лицензиях на DeviceLock.

Настройки сервера

Эти параметры служат для настройки сервера DeviceLock Enterprise Server.



Можно настроить следующие параметры:

- **Администраторы сервера** - Список и права доступа администраторов сервера.
- **Сертификат DeviceLock** - Сертификат DeviceLock для сервера DeviceLock Enterprise Server.

  Подробнее об этих параметрах см. в разделе Администраторы сервера.
- **Учетная запись сервиса при загрузке** - Учетная запись для запуска службы сервера (параметр “Входить в систему как”).
- **TCP-порт** - Порт для подключения консоли к серверу DeviceLock Enterprise Server.

  Подробнее об этих параметрах см. в разделе Учетная запись службы и параметры подключения.
- **Имя базы данных** - Имя базы данных сервера DeviceLock Enterprise Server.
- **Тип соединения** - Определяет драйвер ODBC или системный источник данных для соединения с сервером базы данных DeviceLock Enterprise Server.
- **Имя сервера базы данных** - Имя сервера, управляющего базой данных DeviceLock Enterprise Server. Этот параметр отображается, если выбран тип соединения с использованием драйвера ODBC.
- **Имя пользователя базы данных** - Логин, используемый для доступа к базе данных DeviceLock Enterprise Server. Этот параметр отображается, если для подключения к базе данных требуется логин (например, если выбран режим “Аутентификация SQL Server” или в качестве сервера базы данных используется PostgreSQL).

- **Системный источник данных** - Имя источника данных для доступа к серверу базы данных DeviceLock Enterprise Server. Этот параметр отображается, если выбран тип соединения с использованием системного источника данных.

  Подробнее о параметрах базы данных, см. в разделе Настройка базы данных.

- **Хранить файлы теневого копирования в базе данных** - Режим хранения файлов теневого копирования: в базе данных или на диске.

- **Путь к хранилищу** - Место хранения файлов теневого копирование на диске.

  Подробнее о параметрах хранения файлов см. в разделе Хранить файлы теневого копирования в базе данных.

- **Лицензии DeviceLock** - Просмотр информации, связанной с лицензией DeviceLock, и загрузка лицензии DeviceLock. Подробнее см. в разделе Информация о лицензии.

- **Потоковое сжатие** - Если этот параметр включен, DeviceLock сжимает данные аудита и теневого копирования, передаваемые с сервиса DeviceLock на сервер DeviceLock Enterprise Server. Сжатие данных может существенно снизить нагрузку на сеть.

- **Распаковывать ISO-образы** - Если этот параметр включен, сервер извлекает файлы из CD/DVD/BD-образов во время их теневого копирования.

- **Ограничение размера сессии сбора данных (МБ)** - Если этот параметр включен, сервер ограничивает объем данных, собранных с одного компьютера, что может повысить общую производительность сбора данных.

- **Консолидация журналов** - Позволяет просмотреть или изменить параметры консолидации журналов. Подробнее см. в разделе Консолидация журналов.

Контекстное меню узла **Настройки сервера** содержит следующую команду:

- **Свойства** - Запускает мастер управления параметрами сервера.

Дополнительные сведения см. в разделе Управление настройками сервера.

Администраторы сервера

Узел **Администраторы сервера** определяет список и права доступа администраторов сервера DeviceLock Enterprise Server, а также сертификат DeviceLock, используемый данным сервером.

Контекстное меню этого узла содержит следующую команду:

- **Свойства** - Открывает диалоговое окно, в котором можно настроить список администраторов сервера и установить или удалить сертификат DeviceLock.

См. также:

Администраторы сервера и сертификат

Управление настройками сервера

Используйте контекстное меню, которое появляется при нажатии правой кнопки мыши, или дважды щелкните **Потоковое сжатие**, чтобы включить или выключить этот параметр. Когда параметр **Потоковое сжатие** включен, DeviceLock сжимает данные аудита и теневого копирования, передаваемые сервисом DeviceLock на сервер DeviceLock Enterprise Server. Это позволяет уменьшить размер передаваемых данных и соответственно снизить нагрузку на сеть.

Если включен параметр **Распаковывать ISO-образы**, DeviceLock Enterprise Server автоматически извлекает файлы из CD/DVD/BD-образов в журнале теневого копирования. При этом все файлы из CD/DVD/BD-образов извлекаются по мере поступления образов на сервер и сохраняются в базе данных по отдельности (одна запись на один файл). Если данный параметр выключен, в базе данных сохраняются целиком сами CD/DVD/BD-образы.

Если включен параметр **Ограничение размера сессии сбора данных (МБ)**, DeviceLock Enterprise Server будет скачивать с сервиса DeviceLock данные в объеме, указанном в этом параметре (значение по умолчанию составляет 1024 МБ), после чего агент будет перемещен в конец очереди для скачивания оставшихся данных позже. Этот параметр может быть также использован для повышения скорости сбора данных с агентов, в локальном хранилище которых находится незначительный объем данных, в то время как на некоторых других агентах может храниться существенный объем данных теневого копирования.

Используйте команду **Свойства** из контекстного меню других параметров, чтобы просмотреть или изменить их настройки в открывшемся диалоговом окне. Также можно дважды щелкнуть параметр, чтобы открыть диалоговое окно с его настройками.

Чтобы открыть мастер настройки для пошаговой установки или просмотра параметров сервера, выберите команду **Свойства** из контекстного меню узла **Настройки сервера**. Мастер и соответствующие настройки параметров описаны в разделах, посвященных установке сервера DeviceLock Enterprise Server (см. Учетная запись службы и параметры подключения, Администраторы сервера и сертификат, Информация о лицензии, Настройка базы данных).

Средства просмотра журналов DeviceLock

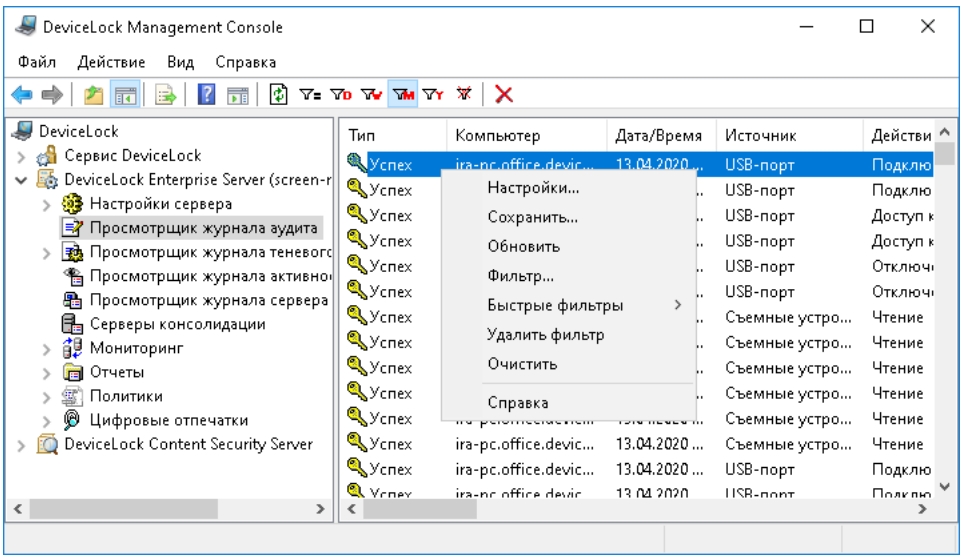
Сервер DeviceLock Enterprise Server предоставляет следующие инструменты для просмотра журналов DeviceLock:

- Просмотрщик журнала аудита (для сервера) - Для просмотра записей аудита, хранимых на сервере DeviceLock Enterprise Server.
- Просмотрщик журнала теневого копирования (для сервера) - Для просмотра данных теневого копирования, хранимых на сервере DeviceLock Enterprise Server.
- Просмотрщик журнала активности пользователей - Для просмотра записей мониторинга пользовательской активности, хранимых на сервере DeviceLock Enterprise Server.
- Просмотрщик журнала сервера - Для просмотра записей внутреннего журнала сервера DeviceLock Enterprise Server.

Просмотрщик журнала аудита (для сервера)

Консоль управления содержит встроенный просмотрщик записей аудита, хранимых на сервере DeviceLock Enterprise Server.

DeviceLock Enterprise Server собирает записи аудита с удаленного компьютера, только если у параметра Тип журнала аудита в настройках сервиса DeviceLock на этом компьютере выбрана опция **Журнал DeviceLock**. В противном случае, записи аудита хранятся в стандартном журнале Windows на локальном компьютере, и для их просмотра следует использовать Просмотрщик журнала аудита (для компьютера).



Разница между просмотрщиком журнала аудита для сервера и для отдельных компьютеров незначительна, поэтому вначале рекомендуем ознакомится с разделом Просмотрщик журнала аудита (для компьютера) данного руководства.

По сравнению с просмотрщиком журнала аудита для отдельных компьютеров, серверный просмотрщик имеет следующие дополнительные столбцы:

- **Компьютер** - Имя компьютера, на котором данное событие было зарегистрировано сервисом DeviceLock.
- **Событие** - Идентификационный номер события.
- **Дата/Время сбора** - Дата и время, когда событие было получено сервером DeviceLock Enterprise Server от сервиса DeviceLock.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, получившего данное событие от сервиса DeviceLock.
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов (см. Консолидация журналов).
- **Сервер консолидации** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов (см. Консолидация журналов).

В столбцах **Причина**, **Имя** и **Информация** могут отображаться дополнительные сведения об устройстве. Консоль извлекает эти сведения из поля “Описание” базы данных USB-устройств. Если не удается получить сведения из поля “Описание”, отображается идентификатор устройства, идентификатор VID и серийный номер или системный идентификатор.

Управление журналом аудита (для сервера)

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узел **DeviceLock Enterprise Server** и щелкните правой кнопкой мыши **Просмотрщик журнала аудита** под этим узлом.

  - или -

- В дереве консоли DeviceLock Management Console выберите **DeviceLock Enterprise Server** > **Просмотрщик журнала аудита** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале (см. Настройки журнала аудита (для сервера)).
- **Сохранить** - Сохранить журнал в указанный файл.
- **Обновить** - Обновить список событий с учетом последних изменений.
- **Фильтр** - Отображать только записи о событиях, которые удовлетворяют заданным условиям (см. Фильтр журнала аудита (для сервера)).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра событий, произошедших за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

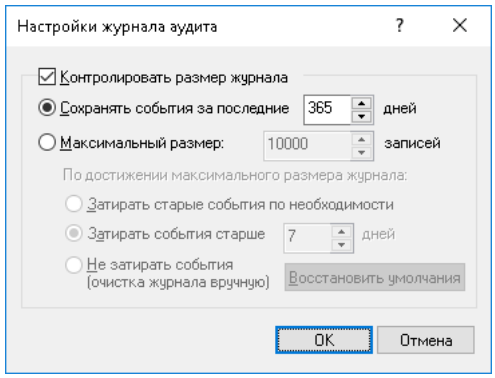
  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).
- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи о событиях, имеющиеся в журнале на данный момент.

  Эта команда добавляет в журнал запись об удалении, указывающую, сколько записей было удалено, а также кто выполнил удаление и с какого компьютера.

Настройки журнала аудита (для сервера)

Чтобы контролировать размер журнала и действия сервера при переполнении журнала, выберите команду **Настройки** в контекстном меню просмотрщика этого журнала в дереве консоли. Затем просмотрите или измените настройки в появившемся диалоговом окне.



Установите флажок **Контролировать размер журнала**, чтобы позволить серверу контролировать количество записей в журнале и удалять устаревшие записи. Если этот флажок не установлен, сервер использует все доступное пространство базы данных для хранения журнала.

Размер журнала может контролироваться сроком хранения или количеством записей:

- **Сохранять события за последние** <число> **дней** - Если выбран этот параметр, в журнале хранятся записи не старше заданного количества дней (по умолчанию - 365 дней).
- **Максимальный размер:** <число> **записей** - Если выбран этот параметр, в журнале хранится не более заданного количества записей. В этом случае необходимо выбрать действие сервера, которое будет выполняться, когда журнал достигнет максимального размера:
  - **Затирать старые события по необходимости** - Новые записи событий продолжают сохраняться при достижении максимального размера журнала. Каждая запись нового события заменяет собой самую старую запись в журнале.
  - **Затирать события старше** <число> **дней** - Новые записи событий заменяют собой только записи, хранящиеся дольше заданного количества дней. Поддерживаемая настройка - до 32 767 дней.
  - **Не затирать события (очистка журнала вручную)** - При достижении максимального размера журнала новые записи событий не добавляются. Чтобы обеспечить их добавление, необходимо очистить журнал вручную.

Примечание: Сервер удаляет старые записи по дате, указанной в столбце **Дата/Время сбора** (если запись была получена непосредственно от сервиса DeviceLock), либо по дате, указанной в столбце **Дата/Время консолидации** (если запись была получена от другого сервера посредством консолидации).

Чтобы использовать настройки по умолчанию, выберите параметр **Максимальный размер** и нажмите кнопку **Восстановить умолчания**. В результате будут установлены следующие настройки:

- Максимальный размер: 10 000 записей
- Затирать события старше 7 дней

Если в журнале аудита нет места для новых записей, и настройки журнала не позволяют удалить старые записи, сервер не удаляет данные аудита с компьютеров пользователей. Это предотвращает потерю данных аудита из-за отсутствия места в журнале. Когда в журнале появляется свободное место, сервер перемещает оставшиеся данные аудита с компьютеров пользователей в этот журнал.

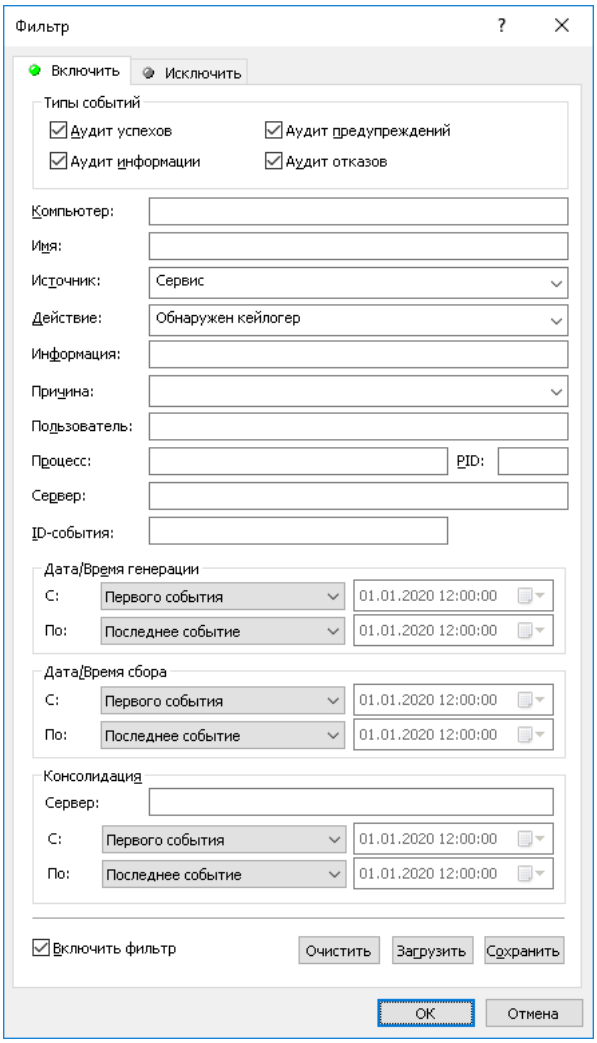
Примечание:

- Фактическое количество записанных в журнале событий может временно превышать предел, заданный в настройках, поскольку для снижения нагрузки на SQL-сервер очистка журнала выполняется не чаще, чем раз в 30 минут.
- Если одна и та же база данных используется несколькими серверами DeviceLock Enterprise Server, то фактическое количество записанных в журнале событий может незначительно превышать предел, заданный в настройках журнала.
- Настройки журнала хранятся в базе данных и относятся к журналу, а не к серверу. У всех серверов DeviceLock Enterprise Server, использующих одну и ту же базу данных, будут одинаковые настройки журнала.

Фильтр журнала аудита (для сервера)

Просмотрщик журнала аудита (для сервера) позволяет отфильтровать данные так, чтобы только записи, удовлетворяющие заданным условиям, выводились в список.

Чтобы открыть диалоговое окно **Фильтр**, выберите команду **Фильтр** из контекстного меню, доступного по нажатию правой кнопки мыши на элементе **Просмотрщик журнала аудита**, или нажмите кнопку ▽ на панели инструментов.



Фильтр журнала аудита для сервера настраивается аналогично фильтру журнала аудита для отдельных компьютеров, описанному в разделе Фильтр журнала аудита (для компьютера).

Чтобы настроить фильтр, установите флажок **Включить фильтр** на соответствующей вкладке в зависимости от того, следует ли настраивать условия включения или исключения.

Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

По сравнению с фильтром журнала аудита для отдельных компьютеров этот серверный фильтр предоставляет следующие дополнительные поля:

- **Компьютер** - Имя компьютера, на котором событие было зарегистрировано сервисом DeviceLock. Это поле нечувствительно к регистру.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, получившего событие от сервиса DeviceLock. Это поле нечувствительно к регистру.
- **ID-события** - Идентификационный номер события. Используя точку с запятой в качестве разделителя, можно задать несколько номеров.
- **Дата/Время генерации** - Настройки временного диапазона для фильтрации событий по времени, когда они были зарегистрированы сервисом DeviceLock.
- **Дата/Время сбора** - Настройки временного диапазона для фильтрации событий по времени, когда они были получены сервером DeviceLock Enterprise Server от сервиса DeviceLock.
- **Консолидация** - Поля для фильтрации по данным, относящимся к консолидации журналов (см. Консолидация журналов):
    - **Сервер** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов. Это поле нечувствительно к регистру и допускает знаки подстановки (* и ?). Используя точку с запятой в качестве разделителя, можно задать несколько значений.
    - **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были последний раз получены с удаленного сервера при консолидации журналов.

Для каждого временного диапазона предусмотрены следующие настройки:

- **С** - Начало диапазона. Возможные значения:
    - **Первого события** - Фильтровать события, начиная с самой ранней даты и времени в соответствующем поле журнала.
    - **События от** - Фильтровать события, начиная с определенной даты и времени.
- **По** - Конец диапазона. Возможные значения:
    - **Последнее событие** - Фильтровать события, заканчивая самой поздней датой и временем в соответствующем поле журнала.
    - **События от** - Фильтровать события, заканчивая определенной датой и временем.

Примечание: Чтобы облегчить настройку фильтра, его строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

Настраивая фильтр, учитывайте следующее:

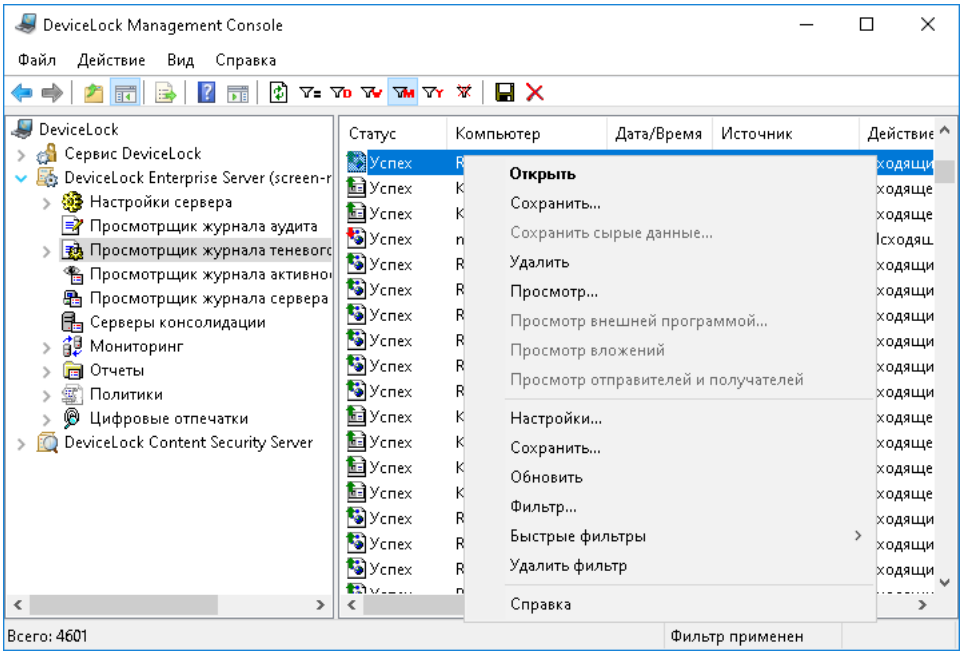
- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

При настройке фильтра по полю **Имя**, **Причина** или **Информация** учитывайте следующее:

- Фильтр применяется к данным, отображаемым в столбцах списка событий. Поскольку в столбцах **Имя**, **Причина** и **Информация** могут содержаться описания устройств, фильтр может оставить в списке (или исключить из списка) устройства, описание которых соответствует условию фильтра по полю **Имя**, **Причина** или **Информация**.
- Событие удовлетворяет условию фильтра, если какая-либо часть данных столбца **Имя**, **Причина** или **Информация** соответствует одноименному полю фильтра. Например, события, у которых в столбце **Имя** указано `USB-устройство (USB-Admin)`, `USB-устройство (Admin)` или `USB-устройство (Administrator)`, удовлетворяют условию фильтра, у которого в поле **Имя** указано `Admin`.
- Применительно к описаниям устройств в столбце **Имя**, **Причина** или **Информация** знаки подстановки * и ? действуют как разделители в соответствующих полях фильтра. Событие соответствует фильтру, если какая-либо часть данных столбца соответствует любой части данных поля фильтра, разделенных символом подстановки. Например, события, у которых описание устройства в столбце **Имя** содержит слово `Admin` или `User` (например, `USB-устройство (Administrator)` или `USB-устройство (USB-User)`), удовлетворяет условиям фильтра, у которого в поле **Имя** указано `User*Admin`.

Просмотрщик журнала теневого копирования (для сервера)

Консоль управления содержит встроенный просмотрщик данных теневого копирования, хранимых на сервере DeviceLock Enterprise Server.



Разница между просмотрщиком журнала теневого копирования для сервера и для отдельных компьютеров незначительна, поэтому рекомендуем вначале ознакомится с разделом Просмотрщик журнала теневого копирования (для компьютера) данного руководства.

По сравнению с просмотрщиком журнала теневого копирования для отдельных компьютеров, серверный просмотрщик имеет следующие дополнительные столбцы:

- **Компьютер** - Имя компьютера, на котором данное событие было зарегистрировано сервисом DeviceLock.
- **Дата/Время сбора** - Дата и время, когда сервер DeviceLock Enterprise Server получил данное событие от сервиса DeviceLock.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, получившего данное событие от сервиса DeviceLock.
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов (см. Консолидация журналов).
- **Сервер консолидации** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов (см. Консолидация журналов).

В столбце **Информация** могут отображаться дополнительные сведения об устройстве. Консоль извлекает эти сведения из поля “Описание” базы данных USB-устройств. Если не удается получить сведения из поля “Описание”, отображается идентификатор устройства, идентификатор VID и серийный номер или системный идентификатор.

Управление записями теневого копирования

Для управления записями теневого копирования служит контекстное меню, появляющееся при нажатии правой кнопки мыши на каждой записи. Меню содержит следующие команды:

- Открыть
- Сохранить
- Сохранить сырые данные
- Удалить
- Просмотр
- Просмотр внешней программой
- Просмотр вложений
- Просмотр отправителей и получателей

При удалении записей в серверном просмотрщике журнала теневые копии файлов удаляются из базы данных или с диска (в зависимости от флага Хранить файлы теневого копирования в базе данных), при этом сведения о каждом удаленном файле (имя файла, размер, пользователь, дата/время и т.п.) заносятся в Журнал удаленных данных теневого копирования.

Журнал удаленных данных теневого копирования используется, когда теневые копии файлов больше не нужны, и требуется очистить хранилище файлов (базу данных на SQL-сервере или папку на диске), но в то же время необходимо сохранить информацию о факте их передачи.

Управление журналом теневого копирования (для сервера)

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узел **DeviceLock Enterprise Server** и щелкните правой кнопкой мыши **Просмотрщик журнала теневого копирования** под этим узлом.

  - или -

- В дереве консоли DeviceLock Management Console выберите **DeviceLock Enterprise Server** > **Просмотрщик журнала теневого копирования** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

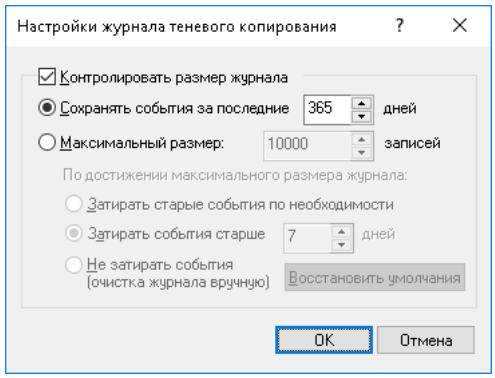
- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале (см. Настройки журнала теневого копирования (для сервера)).
- **Сохранить** - Сохранить журнал в указанный файл.
- **Обновить** - Обновить список записей с учетом последних изменений.
- **Фильтр** - Отображать только записи о событиях, которые удовлетворяют заданным условиям (см. Фильтр журнала теневого копирования (для сервера)).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра записей за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).
- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.

Настройки журнала теневого копирования (для сервера)

Чтобы контролировать размер журнала и действия сервера при переполнении журнала, выберите команду **Настройки** в контекстном меню просмотрщика этого журнала в дереве консоли. Затем просмотрите или измените настройки в появившемся диалоговом окне.



Настройки данного журнала аналогичны настройкам журнала аудита, см. Настройки журнала аудита (для сервера).

Когда в соответствии с настройками журнала серверу требуется удалить старые записи из журнала теневого копирования, эти записи переносятся в Журнал удаленных данных теневого копирования.

Примечание: Сервер удаляет старые записи по дате, указанной в столбце **Дата/Время сбора** (если запись была получена непосредственно от сервиса DeviceLock), либо по дате, указанной в столбце **Дата/Время консолидации** (если запись была получена от другого сервера посредством консолидации).

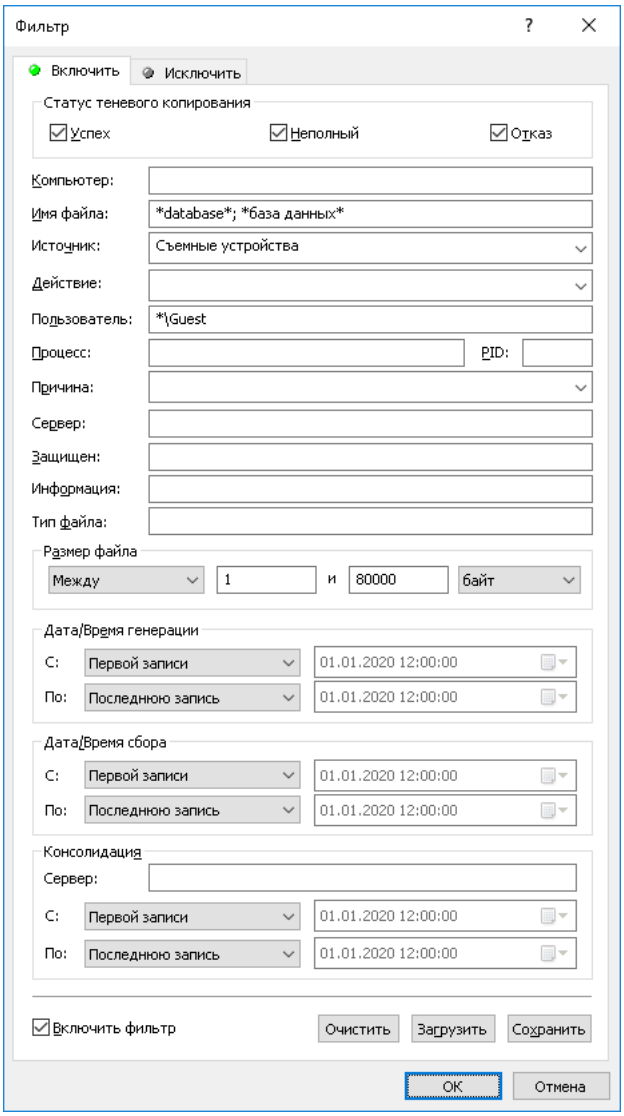
Если в журнале теневого копирования нет места для новых записей, а настройки журнала не позволяют удалить старые записи, сервер не удаляет данные теневого копирования с компьютеров пользователей. Это предотвращает потерю данных теневого копирования из-за отсутствия места в журнале. Когда в журнале появляется свободное место, сервер перемещает оставшиеся данные теневого копирования с компьютеров пользователей в этот журнал.

Мы настоятельно рекомендуем не допускать ситуации, когда большой объем данных теневого копирования скапливается на компьютерах пользователей. Чтобы избежать такой ситуации, необходимо регулярно использовать Просмотрщик журнала сервера для отслеживания предупреждающих записей в журнале сервера DeviceLock Enterprise Server и соответствующим образом корректировать настройки журнала теневого копирования на сервере.

Фильтр журнала теневого копирования (для сервера)

Просмотрщик журнала теневого копирования (для сервера) позволяет отфильтровать данные так, чтобы только записи, удовлетворяющие заданным условиям, выводились в список.

Чтобы открыть диалоговое окно **Фильтр**, выберите команду **Фильтр** из контекстного меню, доступного по нажатию правой кнопки мыши на элементе **Просмотрщик журнала теневого копирования**, или нажмите кнопку ▽= на панели инструментов.



Фильтр журнала теневого копирования для сервера настраивается аналогично фильтру журнала теневого копирования для отдельных компьютеров, описанному в разделе Фильтр журнала теневого копирования (для компьютера).

Чтобы настроить фильтр, установите флажок **Включить фильтр** на соответствующей вкладке в зависимости от того, следует ли настраивать условия включения или исключения.

Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

По сравнению с фильтром журнала теневого копирования для отдельных компьютеров, этот серверный фильтр имеет следующие дополнительные поля:

- **Компьютер** - Имя компьютера, на котором данное событие было зарегистрировано сервисом DeviceLock. Это поле нечувствительно к регистру.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, получившего данное событие от сервиса DeviceLock. Это поле нечувствительно к регистру.
- **Дата/Время генерации** - Настройки временного диапазона для фильтрации событий по времени, когда они были зарегистрированы сервисом DeviceLock.
- **Дата/Время сбора** - Настройки временного диапазона для фильтрации событий по времени, когда они были получены сервером DeviceLock Enterprise Server от сервиса DeviceLock.
- **Консолидация** - Поля для фильтрации по данным, относящимся к консолидации журналов (см. Консолидация журналов):
    - **Сервер** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов. Это поле нечувствительно к регистру и позволяет использовать знаки подстановки (* и ?). Используя точку с запятой в качестве разделителя, можно задать несколько значений.
    - **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были последний раз получены с удаленного сервера при консолидации журналов.

Для каждого временного диапазона предусмотрены следующие настройки:

- **С** - Начало диапазона. Возможные значения:
    - **Первой записи** - Фильтровать события, начиная с самой ранней даты и времени в соответствующем поле журнала.
    - **Записи от** - Фильтровать события, начиная с определенной даты и времени.
- **По** - Конец диапазона. Возможные значения:
    - **Последнюю запись** - Фильтровать события, заканчивая самой поздней датой и временем в соответствующем поле журнала.
    - **Записи от** - Фильтровать события, заканчивая определенной датой и временем.

Примечание: Чтобы облегчить настройку фильтра, его строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

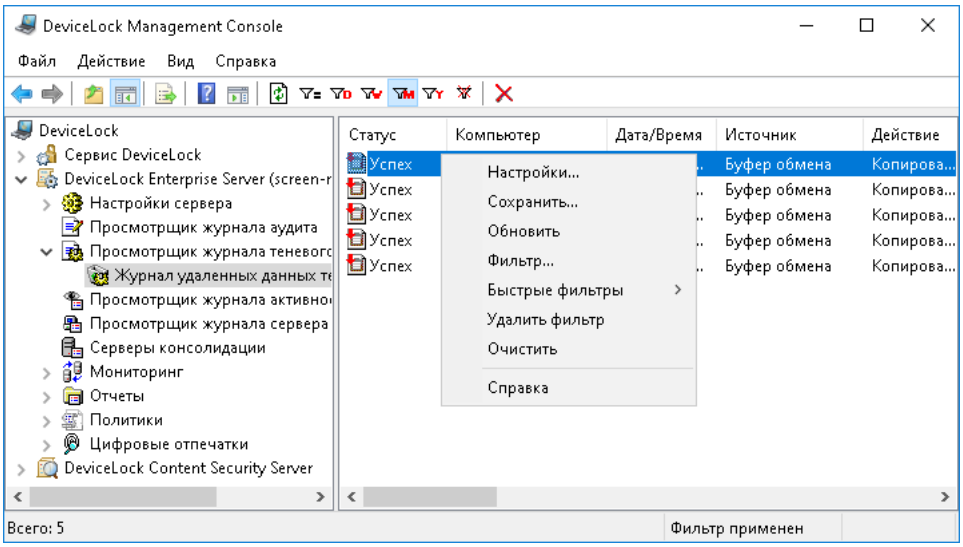
Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

Журнал удаленных данных теневого копирования

Этот встроенный просмотрщик позволяет получить список записей, удаленных из журнала теневого копирования.

Удаление записи из журнала теневого копирования приводит к удалению теневой копии данных; при этом мета-данные (имя и размер файла, имя пользователя, дата/время и т.п.) сохраняются в журнале удаленных данных теневого копирования.



Данный журнал используется, когда теневые копии файлов больше не нужны, и требуется очистить хранилище теневых копий (базу данных на SQL-сервере или папку на диске), но в то же время необходимо сохранить информацию о самом факте передачи данных.

Просмотрщик этого журнала имеет те же столбцы, что и Просмотрщик журнала теневого копирования (для сервера).

Управление журналом удаленных данных теневого копирования

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узлы **DeviceLock Enterprise Server** > **Просмотрщик журнала теневого копирования** и щелкните правой кнопкой мыши **Журнал удаленных данных теневого копирования**.

  - или -

- В дереве консоли DeviceLock Management Console выберите **DeviceLock Enterprise Server** > **Просмотрщик журнала теневого копирования** > **Журнал удаленных данных теневого копирования** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале.

  Настройки данного журнала аналогичны настройкам журнала аудита, см. Настройки журнала аудита (для сервера).

  > **Внимание:** Если в журнале удаленных данных теневого копирования нет места для новых записей, а настройки журнала не позволяют удалить старые записи, сервер будет терять новые записи. Во избежание потери данных из-за отсутствия места в журнале необходимо регулярно использовать Просмотрщик журнала сервера для отслеживания предупреждающих записей в журнале сервера DeviceLock Enterprise Server и соответствующим образом корректировать настройки журнала удаленных данных теневого копирования.

- **Сохранить** - Сохранить журнал в указанный файл.
- **Обновить** - Обновить список записей с учетом последних изменений.
- **Фильтр** - Отображать только записи о событиях, которые удовлетворяют заданным условиям.

  Фильтр данного журнала аналогичен описанному в разделе Фильтр журнала теневого копирования (для сервера).

- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра событий, произошедших за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

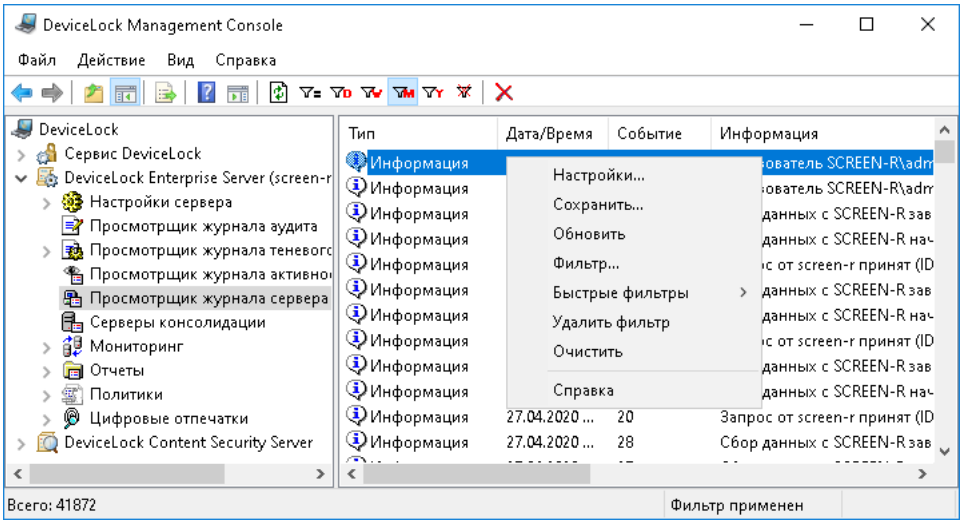
  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).

- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи, имеющиеся в журнале на данный момент.

  Эта команда добавляет в журнал запись об удалении, указывающую, сколько записей было удалено, а также кто выполнил удаление и с какого компьютера.

Просмотрщик журнала сервера

Этот встроенный просмотрщик позволяет получить список записей из внутреннего журнала сервера DeviceLock Enterprise Server. Сервер использует этот журнал, чтобы протоколировать свои собственные события, ошибки и любую другую важную информацию (например, изменения в настройках, запуск и остановку, номер версии и т.п.).



Информация из этого журнала может быть полезной для диагностики и выявления проблем в работе сервера, мониторинга изменений в его настройках и действий по очистке журналов.

Столбцы просмотрщика определены следующим образом:

- **Тип** - Возможны события следующих типов:
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- **Дата/Время** - Дата и время события.
- **Событие** - Идентификационный номер события.
- **Информация** - Прочая информация о данном событии, такая как описание ошибки, имя и значение измененного параметра и т.п.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, на котором данное событие произошло.
- **Запись N** - Порядковый номер записи в списке событий.
- **Сервер консолидации** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов (см. Консолидация журналов).
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов (см. Консолидация журналов).

Управление журналом сервера

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узел **DeviceLock Enterprise Server** и щелкните правой кнопкой мыши **Просмотрщик журнала сервера** под этим узлом.

  - или -

- В дереве консоли DeviceLock Management Console выберите **DeviceLock Enterprise Server** > **Просмотрщик журнала сервера** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды управления журналом (рядом с названием команды показана кнопка панели инструментов, соответствующая этой команде):

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале (см. Настройки журнала сервера).
- **Сохранить** - Сохранить журнал в указанный файл.
- **Обновить** - Обновить список событий с учетом последних изменений.
- **Фильтр** - Отображать только записи о событиях, которые удовлетворяют заданным условиям (см. Фильтр журнала сервера).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра событий, произошедших за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

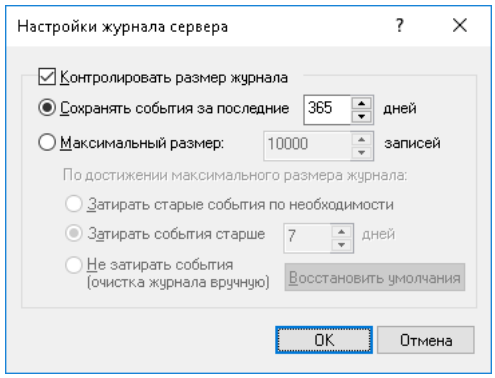
  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).
- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи о событиях, имеющиеся в журнале на данный момент.

  Эта команда добавляет в журнал запись об удалении, указывающую, сколько записей было удалено, а также кто выполнил удаление и с какого компьютера.

Настройки журнала сервера

Чтобы контролировать размер журнала и действия сервера при переполнении журнала, выберите команду **Настройки** в контекстном меню просмотрщика этого журнала в дереве консоли. Затем просмотрите или измените настройки в появившемся диалоговом окне.

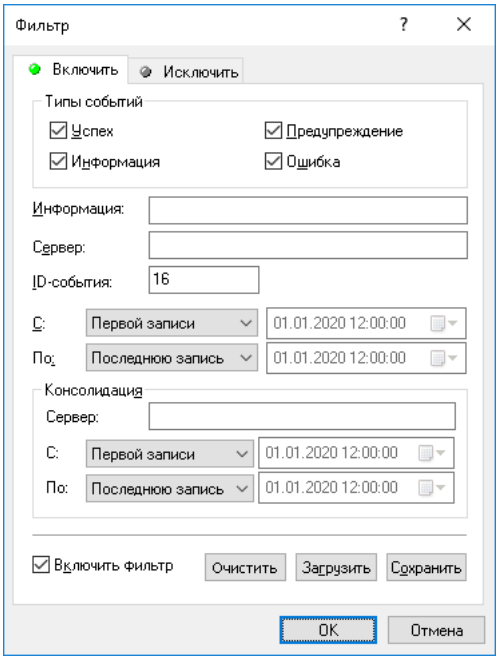


Настройки данного журнала аналогичны настройкам журнала аудита, см. Настройки журнала аудита (для сервера).

Примечание: Сервер удаляет старые записи по дате, указанной в столбце **Дата/Время** (если запись была выполнена локальным сервером), либо по дате, указанной в столбце **Дата/Время консолидации** (если запись была получена от другого сервера посредством консолидации).

Фильтр журнала сервера

Просмотрщик журнала сервера позволяет отфильтровать данные так, чтобы только записи, удовлетворяющие заданным условиям, выводились в список. Чтобы открыть диалоговое окно **Фильтр**, выберите команду **Фильтр** из контекстного меню, доступного по нажатию правой кнопки мыши на элементе **Просмотрщик журнала сервера**, или нажмите кнопку ▽ на панели инструментов.



Фильтр журнала сервера настраивается аналогично фильтру журнала аудита, описанному в разделе Фильтр журнала аудита (для компьютера).

Чтобы настроить фильтр, установите флажок **Включить фильтр** на соответствующей вкладке в зависимости от того, следует ли настраивать условия включения или исключения.

Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

Когда фильтр включен, можно определить условия фильтрации, задав необходимые значения в следующих полях:

- **Типы событий** - Фильтрация по типу событий. Возможны следующие варианты (установите соответствующие флажки):
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- Строковые поля, предназначенные для включения или исключения из списка записей о событиях, у которых в указанном поле данных встречается заданная строка. Например, для фильтрации записей по имени сервера, на котором произошло событие, задайте строку фильтра в поле **Сервер**. Для фильтрации записей о событиях с определенными ID-номерами, введите номера искомых событий в поле **ID-события**, разделяя их точкой с запятой.

Предусмотрены следующие строковые поля:

- **Информация** - Расширенная информация о событии, такая как описание ошибок, имя и значение измененных параметров сервера и т.п.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, на котором произошло событие.
- **ID-события** - Идентификационный номер события.

- **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были зарегистрированы сервером.
- **Консолидация** - Поля для фильтрации по данным, относящимся к консолидации журналов (см. Консолидация журналов):
  - **Сервер** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов. Это поле нечувствительно к регистру и позволяет использовать знаки подстановки (* и ?). Используя точку с запятой в качестве разделителя, можно задать несколько значений.
  - **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были последний раз получены с удаленного сервера при консолидации журналов.

Для каждого временного диапазона предусмотрены следующие настройки:

- **С** - Начало диапазона. Возможные значения:
  - **Первой записи** - Фильтровать события, начиная с самой ранней даты и времени в соответствующем поле журнала.
  - **Записи от** - Фильтровать события, начиная с определенной даты и времени.
- **По** - Конец диапазона. Возможные значения:
  - **Последнюю запись** - Фильтровать события, заканчивая самой поздней датой и временем в соответствующем поле журнала.
  - **Записи от** - Фильтровать события, заканчивая определенной датой и временем.

Примечание: Чтобы облегчить настройку фильтра, его строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

Консолидация журналов

В целях балансировки нагрузки, улучшения производительности и отказоустойчивости крупные организации часто развертывают несколько серверов DeviceLock Enterprise Server для сбора данных из клиентских журналов сервиса DeviceLock. Если серверы при этом не используют общую базу данных SQL, сведения о действиях различных пользователей и клиентских компьютеров будут храниться на разных серверах. Такое распределенное хранение данных может задерживать проведение расследований и составление отчетов, когда требуется полный набор данных в отношении всех пользователей и компьютеров. Там, где невозможно или нецелесообразно использовать общую базу данных для всех серверов DeviceLock Enterprise Server, DeviceLock позволяет решить проблему хранения информации на нескольких серверах с автономными базами данных путем пересылки журналов с отдельных серверов на "центральный собирающий сервер" для их консолидации.

Центральный собирающий DeviceLock Enterprise Server может быть использован в качестве централизованного хранилища журналов DeviceLock с других серверов, называемых удаленными серверами. Удаленные серверы могут отправлять копии своих журналов на центральный сервер по расписанию. Параметры конфигурации позволяют выбирать журналы и задавать расписание их отправки. Центральный сервер можно разместить на локальном компьютере или в облаке (см. Приложение: Консолидация журналов в облаке с помощью OpenVPN).

Консолидация журналов дает возможность реализовать сценарий управления и передачи данных, в котором удаленные серверы накапливают журналы в рабочее время, а ночью отправляют накопленные данные на центральный собирающий сервер. Так, организации с филиалами в разных географических областях могут развернуть серверы в своих филиалах для местного сбора данных в рабочее время и последующей пересылки журналов на центральный сервер после рабочего дня. Основным преимуществом такого развертывания является то, что сбор и пересылка журналов не перегружают каналы связи с филиалами в рабочее время. Ночью, когда каналы связи в основном простаивают, имеет смысл пересылать данные журналов с удаленных серверов на центральный собирающий сервер. В результате центральный сервер собирает журналы со всех филиалов без негативного влияния на каналы сетевой связи, и каждое утро полный набор необходимых данных оказывается доступным для целей расследования и отчетности.

Дальнейшие сведения см. в разделе Приступая к работе с консолидацией журналов.

Приступая к работе с консолидацией журналов

Чтобы настроить консолидацию журналов, администратор DeviceLock Enterprise Server должен сначала решить, какой сервер будет центральным, а затем настроить другие, удаленные серверы для пересылки журналов на центральный сервер.

На каждом сервере, предназначенном для пересылки журналов на центральный сервер, необходимо настроить параметры консолидации журналов, указав:

- Имя компьютера, на котором работает центральный сервер DeviceLock Enterprise Server.
- Расписание отправки журналов на центральный сервер.
- Какие журналы отправляются на центральный сервер.
- Копировать или перемещать данные журналов (в последнем случае данные не будут сохраняться на удаленном сервере).
- Следует ли ограничивать использование пропускной способности сети для передачи журналов на центральный сервер.

При настройке консолидации журналов необходимо также указать способ аутентификации между удаленным сервером и центральным сервером. Предусмотрены следующие способы аутентификации:

- По сертификату (рекомендуемый способ, см. Сертификаты DeviceLock) - Секретный ключ сертификата должен быть установлен на центральном сервере с помощью параметра “Сертификат DeviceLock” в разделе Настройки сервера. Открытый ключ этого сертификата нужно предоставить вместе с именем центрального сервера в настройках консолидации журналов на удаленном сервере.

  Можно также установить секретный ключ сертификата центрального сервера на удаленном сервере, используя для этого параметр “Сертификат DeviceLock” в разделе Настройки сервера. В таком случае открытый ключ на удаленном сервере не требуется.
- По учетной записи Windows - Служба Windows “DeviceLock Enterprise Server” на центральном сервере должна работать под учетной записью с правами администратора DeviceLock Enterprise Server на удаленном сервере.

Для просмотра всех удаленных серверов, отправляющих свои журналы на центральный сервер, используется список DeviceLock Enterprise Server > Серверы консолидации в консоли, подключенной к центральному серверу. В этом списке отображаются имена удаленных серверов, расписание отправки журналов на центральный сервер, текущий статус каждого сервера, а также объемы данных, переданных на центральный сервер.

Управление консолидацией журналов

Администратор может настроить DeviceLock Enterprise Server для консолидации журналов DeviceLock на центральном сервере. Для этого в консоли DeviceLock Management Console предоставляются следующие элементы управления:

- Параметры консолидации журналов - На удаленном сервере можно просматривать и изменять параметры подключения к центральному серверу, такие как имя сервера, настройки аутентификации, выбор и расписание отправки журналов и другие параметры.
- Список серверов консолидации - На центральном сервере можно просматривать сведения об удаленных серверах, отправляющих свои журналы на этот сервер, в том числе имена серверов, состояние и расписание передачи журналов, а также объемы передаваемых и ожидающих передачи данных.

Параметры консолидации журналов

Чтобы настроить удаленный сервер DeviceLock Enterprise Server для пересылки журналов на центральный сервер, используется параметр **Консолидация журналов** в разделе **DeviceLock Enterprise Server** > **Настройки сервера** консоли DeviceLock Management Console, подключенной к удаленному серверу. Команда **Свойства** этого параметра открывает диалоговое окно со следующими параметрами:

- **Сервер консолидации** - Имя или IP-адрес компьютера, на котором работает центральный сервер DeviceLock Enterprise Server. В этом поле можно указать только один компьютер.
- **Установить параметры доступа** - Открывает диалоговое окно для настройки аутентификации между удаленным сервером и центральным сервером. Подробнее см. в разделе Настройка аутентификации.
- **Расписание** - Следующие параметры используются для настройки расписания отправки журналов с данного сервера на центральный сервер:
    - **Ежечасно** - Ежечасная отправка. Необходимо задать дату и время начала отправки журналов, а также интервал их отправки. Например, значение 1 вызывает отправку каждый час, а значение 2 - через час.
    - **Ежедневно** - Ежедневная отправка. Необходимо задать дату и время начала отправки журналов, а также интервал их отправки. Например, значение 1 вызывает отправку каждый день, а значение 2 - через день. Отправка происходит ежедневно в заданное время.
    - **Еженедельно** - Еженедельная отправка. Необходимо задать дату и время начала отправки журналов, дни недели, по которым она будет выполняться, а также интервал отправки. Например, значение 1 вызывает отправку каждую неделю, а значение 2 - через неделю. Отправка происходит в заданное время в каждый из указанных дней недели.
    - **Ежемесячно** - Ежемесячная отправка. Необходимо указать месяцы, недели месяца и дни недели для каждого месяца, по которым будет выполняться отправка журналов. Можно также настроить отправку в определенный последний день недели каждого месяца.
- **Прекратить передачу данных через** <число> **ч.** / **дн.** - Если этот флажок установлен, передача журналов прекращается спустя заданное время после ее начала, даже если удаленный сервер не успел передать все имеющиеся у него данные журналов. Данные, которые не были переданы, сохраняются на удаленном сервере для отправки во время следующего сеанса передачи журналов по расписанию.

- **Журналы** - Выбор журналов для передачи на центральный сервер. Передаваться будут только те журналы, рядом с именем которых установлен флажок.
- **Режим консолидации** - Следующие параметры указывают, следует ли перемещать или только копировать данные журналов при их консолидации:
  - **Полный** - Записи журналов, переданные на центральный сервер, не сохраняются на удаленном сервере. Записи журнала теневого копирования на этом сервере удаляются безвозвратно без перемещения в журнал удаленных данных теневого копирования.
  - **Копия** - Записи журналов, переданные на центральный сервер, остаются в журналах на удаленном сервере.
    - **Только имена файлов** - Этот флажок влияет только на передачу данных теневого копирования. Если флажок установлен, из журнала теневого копирования на центральный сервер передаются имена файлов, а сами файлы и другие данные теневого копирования остаются только на удаленном сервере.

Примечание:

- Переключение режима консолидации с **Копия** на **Полный** приводит к тому, что на удаленном сервере стираются все записи журналов, которые ранее были скопированы на центральный сервер.
- При переключении режима консолидации с **Копия** | **Только имена файлов** на **Полный** выполняется копирование недостающих файлов и данных с удаленного сервера на центральный сервер, а затем эти файлы и данные стираются на удаленном сервере.

- **Приоритет трафика** - Следующие параметры указывают, будет ли ограничиваться использование пропускной способности сети для передачи журналов на центральный сервер:
  - **Высокий** - Использовать всю доступную пропускную способность сети.
  - **Средний** - Использовать не более 50% пропускной способности сети.
  - **Низкий** - Использовать не более 20% пропускной способности сети.
- **Дополнительные настройки** - Открывает диалоговое окно для настройки повторных попыток обмена данными при сбоях в канале связи между серверами консолидации. Подробнее см. в разделе Параметры повтора.
- **Тестировать соединение** - Нажмите эту кнопку, чтобы проверить, может ли удаленный сервер с текущими настройками установить соединение с центральным сервером. Если установить соединение не удается, появляется сообщение об ошибке, указывающее причину сбоя. В противном случае появится окно с сообщением о том, что соединение успешно установлено.

Настройка аутентификации

Если в диалоговом окне управления параметрами консолидации нажать кнопку **Установить параметры доступа**, появляется диалоговое окно с параметрами аутентификации между удаленным сервером и центральным сервером:

- **Имя сертификата** - Открытый ключ сертификата DeviceLock (см. Сертификаты DeviceLock) для аутентификации центрального сервера. Секретный ключ этого же сертификата должен быть установлен на центральном сервере с помощью параметра "Сертификат DeviceLock" в разделе Настройки сервера.

  Открытый ключ можно установить в диалоговом окне, которое появляется по нажатию кнопки ... рядом с полем **Имя сертификата**. Кнопка **Удалить** позволяет удалить открытый ключ с данного сервера.

Устанавливать открытый ключ не требуется, если выполнено любое из следующих условий:

- Служба Windows "DeviceLock Enterprise Server" на центральном сервере работает под учетной записью с правами администратора DeviceLock Enterprise Server на удаленном сервере.
- Секретный ключ одного и того же сертификата установлен как на центральном сервере, так и на удаленном сервере с помощью параметра "Сертификат DeviceLock" в разделе Настройки сервера.

Параметры повтора

Если в диалоговом окне управления параметрами консолидации журналов нажать кнопку **Дополнительные настройки**, появляется диалоговое окно с параметрами повтора попыток обмена данными при сбоях в канале связи между серверами консолидации:

- **Количество повторов** - Задает максимальное число повторных попыток обмена данными в ситуации, когда удаленный сервер не может связаться с центральным сервером или центральный сервер не может собрать журналы с удаленного сервера. Если для этого параметра установлено значение `0`, повторных попыток обмена данными не производится.
- **Таймаут попыток** - Задает промежуток времени между последовательными попытками обмена данными между серверами. В случае сбоя связи сервер ожидает заданное количество секунд, прежде чем повторить попытку обмена данными.

У разных удаленных серверов могут быть различные параметры повтора. Удаленный сервер использует свои параметры повтора при отправке запроса консолидации на центральный сервер. Если запрос проходит успешно, эти же параметры затем используются центральным сервером при сборе журналов с соответствующего удаленного сервера.

При настройке параметров повтора примите во внимание, как повторные попытки обмена данными связаны с регулярным сбором журналов по расписанию:

- Счет повторных попыток сбрасывается только после успешного обмена данными. Если было выполнено заданное количество повторов, и все они не были успешными, то до тех пор, пока журналы не будут успешно переданы на центральный сервер, попытки их передачи происходят только по расписанию, без повторов в случае сбоя связи между серверами. Повторы могут быть возобновлены только после успешного сбора журналов.
- Регулярный сбор журналов по расписанию имеет приоритет над повторными попытками. Если повторная попытка запланирована на более позднее время, чем начало регулярного сеанса передачи журналов, сеанс начнется в соответствии с расписанием, независимо от запланированной повторной попытки. В этом случае, если сеанс завершится неудачно, повторная попытка произойдет по истечении таймаута попыток после начала сеанса.

Список серверов консолидации

Серверы, которые заявили о себе как удаленные серверы для данного центрального сервера DeviceLock Enterprise Server, перечисляются в консоли DeviceLock Management Console, подключенной к центральному серверу. Список появляется на панели сведений, если в дереве консоли выбрать **DeviceLock Enterprise Server** > **Серверы консолидации**, и предоставляет следующую информацию о каждом удаленном сервере:

- **Имя** - Имя компьютера, на котором работает удаленный сервер.
- **Статус** - Одно из следующих значений:
  - **Передача** - Выполняется передача журналов с данного сервера на центральный сервер.
  - **Завершено** - Журналы с данного сервера успешно переданы на центральный сервер.
  - **Лицензия недоступна** - Центральный сервер не может получить журналы аудита и/или теневого копирования с данного сервера из-за недостатка лицензий. Для успешной консолидации журналов количество лицензий на центральном сервере должно быть не меньше общего количества клиентских компьютеров, журналы которых передаются на удаленные серверы.
  - **Вне расписания** - Центральный сервер не смог установить связь с данным сервером в запланированные дату и время передачи журналов.
  - **Ошибка** - Центральный сервер не смог получить журналы с данного сервера из-за ошибки.

  Примечание: Значения статуса **Вне расписания** и **Ошибка** указывают на сбой передачи журналов с удаленного сервера. Дата и время последней успешной передачи отображается в столбце **Последний сеанс**. Дополнительные сведения о причинах сбоя можно найти в событии ошибки, зарегистрированном на удаленном и/или центральном сервере (см. Просмотрщик журнала сервера).

- **Расписание** - Очередная запланированная дата и время передачи журналов этим удаленным сервером.
- **Последний сеанс** - Дата и время завершения последнего сеанса передачи журналов этим удаленным сервером.
- **Всего получено** - Общее количество данных, полученных центральным сервером от этого удаленного сервера в течение всего времени.
- **Получено за сеанс** - Количество данных, полученных центральным сервером от этого удаленного сервера в текущем или последнем завершенном сеансе передачи журналов.
- **Осталось получить** - Количество оставшихся данных, которые центральный сервер ожидает получить от этого удаленного сервера.

Примечание: Информация о количестве данных обновляется только в начале сеанса передачи журналов, во время сеанса и непосредственно по его завершении. В промежутках между сеансами отображается информация по состоянию на конец последнего завершенного сеанса передачи журналов.

В контекстном меню на каждом из перечисленных удаленных серверов предоставляются следующие команды:

- **Подключиться к DeviceLock Enterprise Server** - Подключить консоль к данному удаленному серверу.
- **Настройки консолидации журналов** - Открыть диалоговое окно для просмотра и настройки параметров консолидации журналов на данном удаленном сервере.
- **Обновить** - Обновить список удаленных серверов с учетом последних изменений.
- **Удалить** - Не показывать выбранный сервер в списке. Все ранее собранные с этого сервера данные журналов остаются на центральном сервере. Если скрытый этой командой сервер представит новые данные для консолидации, он снова появится в списке.

Дополнительные сведения см. в разделе Консолидация журналов.

Мониторинг

Централизованный мониторинг - функция сервера DeviceLock Enterprise Server, позволяющая контролировать текущее состояние сервиса DeviceLock на удаленных компьютерах путем периодического опроса. Результаты мониторинга отображаются в консоли управления в режиме реального времени, а также сохраняются в специальном журнале для последующего просмотра и анализа (см. Просмотрщик журнала мониторинга).

Кроме того, DeviceLock Enterprise Server периодически сравнивает текущие политики безопасности (настройки) агентов на указанных администратором компьютерах с эталонными политиками, и фиксирует информацию о выявленных отклонениях.

Функция мониторинга в сервере DeviceLock Enterprise Server позволяет устанавливать сервис DeviceLock на контролируемые компьютеры, что можно рассматривать как еще один способ развертывания сервиса DeviceLock в дополнение к традиционным методам (инсталляция ПО через GPO, Microsoft SCCM, через консоли управления DeviceLock, интерактивную установку, и т.д.). Подробнее см. в разделе Установка с помощью DeviceLock Enterprise Server.

Также эту функцию можно использовать как альтернативный способ развертывания настроек, разрешений, аудита, правил теневого копирования и тревожных оповещений на удаленные сетевые компьютеры, которые контролируются сервисом DeviceLock.

Все действия, связанные с мониторингом, выполняются задачами. Список задач можно увидеть на панели сведений при выборе узла **Мониторинг** в дереве консоли. Управление задачами предполагает:

- Создание задачи - Щелкните узел **Мониторинг** правой кнопкой мыши и выберите команду **Создать задачу**.
- Редактирование существующей задачи - Щелкните задачу правой кнопкой мыши и выберите команду **Редактировать задачу**.
- Управление списком компьютеров существующей задачи - Щелкните задачу правой кнопкой мыши и выберите команду **Редактировать список компьютеров**. Эта команда появляется в меню только для задач со статическим списком компьютеров.

  Подробнее см. в разделе Создание/Редактирование задачи.
- Немедленное исполнение задачи - Щелкните задачу правой кнопкой мыши и выберите команду **Запустить сейчас**.
- Просмотр компьютеров, контролируемых определенной задачей - Разверните узел **Мониторинг** и выберите задачу в дереве консоли. Список компьютеров появится на панели сведений. Подробнее см. в разделе Задача и ее контролируемые компьютеры.

  При необходимости, можно подключить консоль к сервису DeviceLock на контролируемом компьютере: щелкните правой кнопкой мыши компьютер в списке и выберите команду **Подключиться к сервису DeviceLock**.
- Удаление задачи - Щелкните задачу правой кнопкой мыши и выберите команду **Удалить задачу**.

Задачи мониторинга

Все действия, связанные с мониторингом, выполняются задачами. На одном сервере DeviceLock Enterprise Server можно создать любое количество задач. Максимальное количество задач на сервере ограничено только количеством свободной памяти, скоростью процессора и пропускной способностью сети. Имейте в виду, что сервер должен иметь достаточно ресурсов, чтобы одновременно подключаться как минимум к 10 удаленным компьютерам.

По умолчанию DeviceLock Enterprise Server может выполнять одновременно до 30 задач. Это означает, что если у вас, например, 40 задач, и все они запускаются в одно и то же время, то сначала будут запущены первые 30 задач, а затем, по мере их окончания, по одной будут запускаться оставшиеся 10 задач.

Тем не менее, максимальное количество одновременно запускаемых задач можно изменить. Для этого добавьте следующее значение в реестр компьютера, на котором работает сервер DeviceLock Enterprise Server:

- Ключ: `HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer`
- Значение: `ConcurrentJobs=dword:<количество_потоков>`

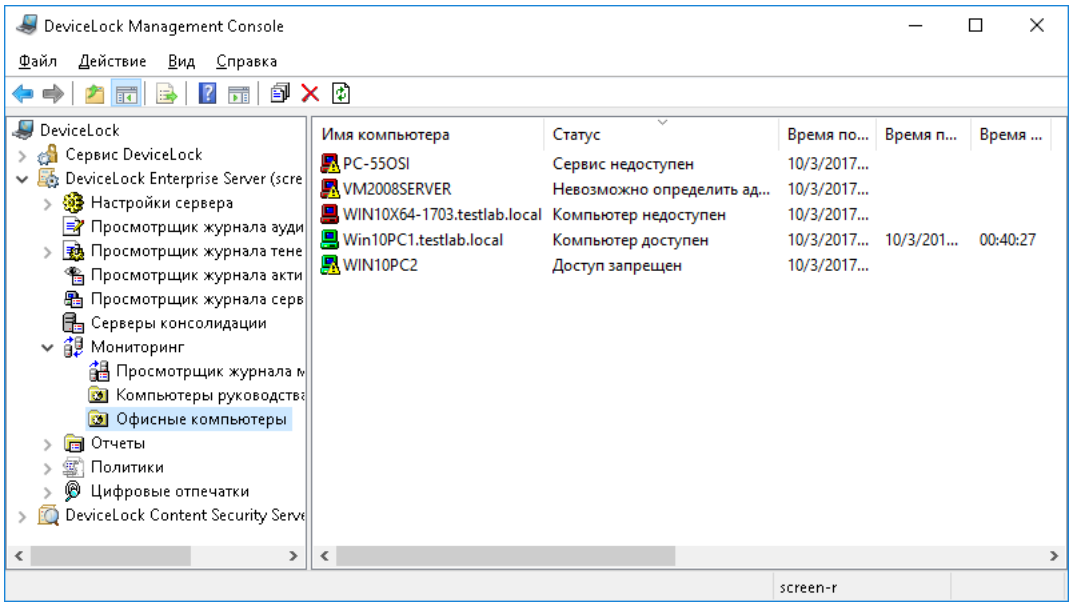
Здесь `<количество_потоков>` должно быть целым числом от 1 до 1000.

Во время своего выполнения задачи пишут полезную информацию в журнал мониторинга (см. раздел Просмотрщик журнала мониторинга). Эта информация включает в себя текущие состояния компьютеров и экземпляров сервиса DeviceLock, а также возможные ошибки, которые возникают в процессе сканирования компьютеров и подключения к экземплярам сервиса DeviceLock.

Также задачи отображают списки компьютеров и их текущие состояния в консоли управления. Это позволяет анализировать ситуацию в режиме реального времени.

Задача и ее контролируемые компьютеры

Задачи мониторинга отображаются в дереве консоли под узлом **DeviceLock Enterprise Server** > **Мониторинг** > **Задачи**.



Выбрав задачу в дереве консоли, можно увидеть список всех компьютеров, контролируемых этой задачей. Чтобы обновить информацию в списке компьютеров, щелкните задачу правой кнопкой мыши и выберите команду **Обновить**.

Панель сведений консоли отображает список контролируемых компьютеров со следующими сведениями по каждому компьютеру:

- **Имя компьютера** - Имя, идентифицирующее компьютер.
- **Статус** - Текущее состояние компьютера и сервиса DeviceLock на этом компьютере.

  Для индикации статуса служит также значок рядом с именем компьютера:

  - Зеленый компьютер - Означает, что компьютер и сервис DeviceLock работают.
  - Красный компьютер - Означает, что компьютер не работает (либо не найден), или работает, но сервис DeviceLock не запущен.
  - Компьютер с восклицательным знаком - Обнаружены проблемы либо с самим компьютером, либо с сервисом DeviceLock на этом компьютере.

  Предусмотрено восемь различных состояний (статусов):

  - **Компьютер доступен** - Компьютер работает и сервис DeviceLock на нем запущен. Также, если эта задача проверяет целостность политики, то данная проверка прошла без ошибок. Значок компьютера в этом случае - "зеленый компьютер".

    Если эта задача восстанавливает измененную политику, иконка компьютера будет - "зеленый компьютер с восклицательным знаком".

  - **Компьютер недоступен** - DeviceLock Enterprise Server не может выполнить сканирование данного компьютера. Это происходит, когда компьютер выключен или соединения блокируются файрволом, но при этом имя компьютера или его IP-адрес могут быть получены через DNS. Значок компьютера в этом случае - "красный компьютер".
  - **Сервис недоступен** - DeviceLock Enterprise Server не может подключиться к сервису DeviceLock. Это происходит, когда компьютер работает, но сервис DeviceLock на нем не запущен. Также это может происходить из-за того, что сервис DeviceLock запущен не на том TCP-порту, который указан в настройках задачи, или соединения блокируются файрволом. Значок компьютера в данном случае - "красный компьютер с восклицательным знаком". Подробнее о проблемах подключения см. в описании параметра Настройки соединения сервиса.
  - **Настройки повреждены** - Компьютер работает и сервис DeviceLock на нем запущен, но некоторые настройки сервиса DeviceLock на этом компьютере отличаются от эталонной политики, заданной в задаче мониторинга (см. описание параметра Проверять настройки сервиса). Значок компьютера в этом случае - зеленый компьютер с восклицательным знаком.

    Щелкните компьютер правой кнопкой мыши и выберите пункт **Просмотр деталей** для просмотра настроек сервиса DeviceLock на контролируемом компьютере, которые отличаются от эталонной политики. Команда **Просмотр деталей** отображает диалоговое окно со списком настроек, не соответствующих эталонной политике. Каждая такая настройка сопровождается описанием несоответствия, например:

    - **отсутствует** - Настройка задана в эталонной политике, но отсутствует на контролируемом компьютере.
    - **отличается** - Настройка задана по-разному в эталонной политике и на контролируемом компьютере.
    - **избыточно** - Настройка отмечена как удаленная в эталонной политике, но задана на контролируемом компьютере.

- **Невозможно определить адрес компьютера** - DeviceLock Enterprise Server не может получить имя/адрес компьютера. Это происходит, когда задано имя компьютера не существующее в DNS. Также это может происходить из-за того, что компьютер в данный момент не включен, а в сети нет DNS-сервера. В таком случае статус **Невозможно определить адрес компьютера** должен трактоваться вами как **Компьютер недоступен**. Значок компьютера в этом случае - "красный компьютер с восклицательным знаком".
- **Неподдерживаемая версия сервиса** - DeviceLock Enterprise Server пытается получить политику (настройки) от сервиса DeviceLock версии 6.2 и ниже. Проверка целостности политик поддерживается только для версий 6.2.1 и выше. Значок компьютера в этом случае - "зеленый компьютер с восклицательным знаком".
- **Доступ запрещён** - DeviceLock Enterprise Server не может подсоединиться к сервису DeviceLock из-за недостатка привилегий. Это происходит, когда учетная запись, под которой запущена служба DeviceLock Enterprise Server, не имеет прав доступа для подключения к сервису DeviceLock. Значок компьютера в этом случае - "зеленый компьютер с восклицательным знаком". Подробнее см. в описании параметра Настройки соединения сервиса.
- **Лицензия недоступна** - Из-за нехватки лицензий DeviceLock Enterprise Server не может провести мониторинг компьютера с работающим сервисом DeviceLock . DeviceLock Enterprise Server контролирует столько экземпляров сервиса DeviceLock, сколько лицензий установлено на DeviceLock Enterprise Server. Для получения дополнительной информации, см. Информация о лицензии в разделе Установка DeviceLock Enterprise Server. Значок компьютера в этом случае - "зеленый компьютер с восклицательным знаком".

Эти статусы (за исключением статуса **Компьютер доступен**) также записываются в журнал мониторинга (см. раздел Просмотрщик журнала мониторинга) и могут быть проанализированы позже.

- **Время последнего сканирования** - Дата и время последней попытки сканирования. Попытка сканирования может быть успешной или неудачной.
- **Время последнего успешного сканирования** - Дата и время последней успешной попытки сканирования.
- **Время работы сервиса** - Время непрерывной работы сервиса DeviceLock.
- **Время работы компьютера** - Время непрерывной работы компьютера, который отслеживается. Сравнив время непрерывной работы компьютера с временем работы сервиса (см. выше), можно определить, останавливался ли сервис DeviceLock в текущем сеансе.
- **Версия сервиса** - Версия сервиса DeviceLock. Последние пять цифр обозначают номер сборки.

Алгоритм мониторинга

Для мониторинга используется простой и эффективный алгоритм:

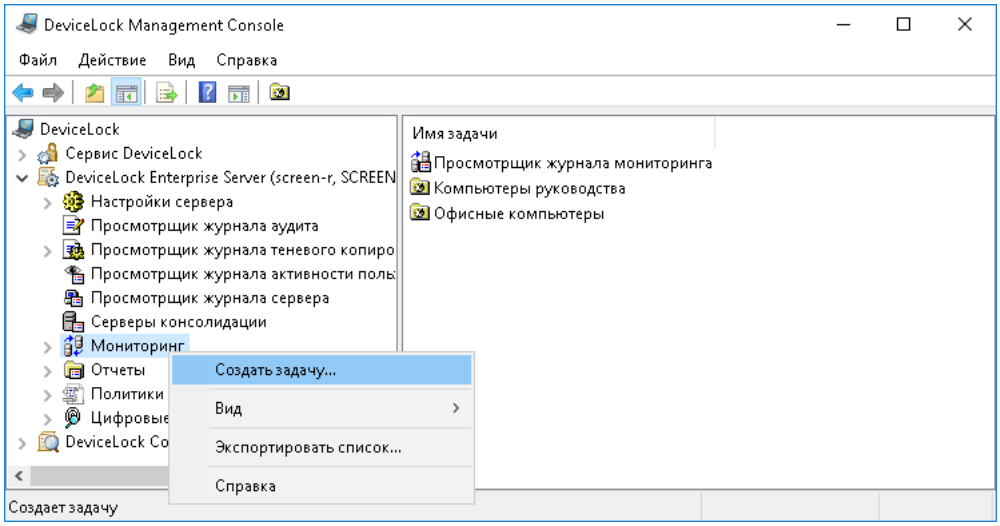
1. Прежде всего DeviceLock Enterprise Server пытается сканировать компьютер и определить, работает он или нет. Если сканирование удалось, то компьютер получает статус **доступен** и мониторинг компьютера продолжается. В противном случае компьютер получает статус **недоступен** и мониторинг компьютера прекращается (происходит запись в журнал).
2. Затем DeviceLock Enterprise Server пытается подключиться к сервису DeviceLock. Если сканирование удалось, то компьютер получает статус **доступен** и мониторинг компьютера продолжается. В противном случае сервис DeviceLock получает статус **недоступен** и мониторинг компьютера прекращается (происходит запись в журнал).
3. Если данная задача должна проверять целостность политики, то мониторинг компьютера продолжается. В противном случае мониторинг компьютера прекращается (в журнал ничего не пишется).
4. DeviceLock Enterprise Server получает политику от сервиса DeviceLock и сравнивает ее с эталонной политикой, присвоенной данной задаче. Если расхождений в политиках не обнаружено, то мониторинг компьютера прекращается (в журнал ничего не пишется). Если обнаружены различия в двух политиках, то мониторинг компьютера продолжается (происходит запись в журнал).
5. Если данная задача должна восстанавливать измененную политику, то DeviceLock Enterprise Server заменяет политику на сервисе DeviceLock на эталонную и мониторинг компьютера прекращается (происходит запись в журнал). В противном случае мониторинг компьютера просто прекращается (в журнал ничего не пишется).

Если на каком либо из шагов, описанных выше, происходит ошибка, то в журнал записывается сообщение об этой ошибке. Если ошибка не критичная, то мониторинг компьютера продолжится. Если же ошибка критичная, то мониторинг компьютера прекратится.

Также, некоторые очень критичные ошибки (такие как нехватка памяти) могут вызвать остановку исполнения всей задачи.

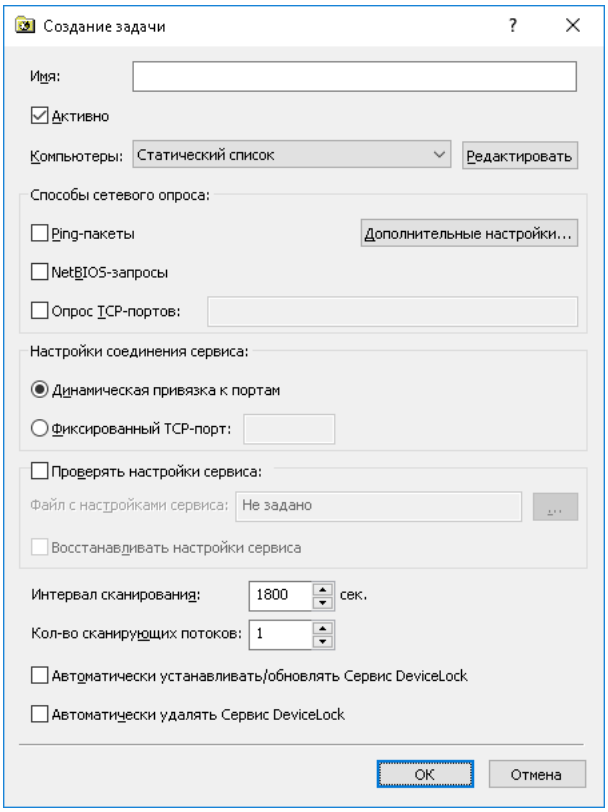
Создание/Редактирование задачи

Каждая задача содержит свой собственный список компьютеров и набор настроек.



Чтобы создать новую задачу, используйте команду **Создать задачу** из контекстного меню, доступного для пункта **Мониторинг**. Чтобы отредактировать существующую задачу, используйте команду **Редактировать задачу** из контекстного меню. Если требуется безвозвратно удалить задачу, выделите эту задачу в дереве консоли и выберите команду **Удалить задачу** из контекстного меню.

Для создания или редактирования задачи используется следующее диалоговое окно:

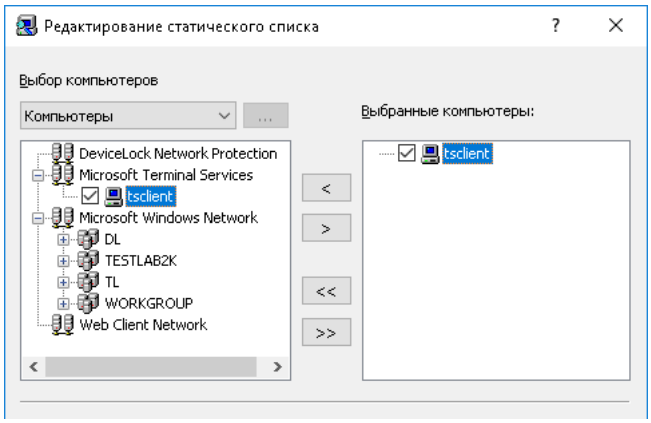


- **Имя** - Имя задачи, которое служит для ее идентификации в списке задач и в журнале мониторинга (см. раздел Просмотрщик журнала мониторинга).
- **Активно** - Если этот флажок установлен, DeviceLock Enterprise Server будет выполнять задачу. Снимите этот флажок, если нужно отключить выполнение данной задачи без ее удаления.
- **Компьютеры** - Тип списка компьютеров, используемый для задания компьютеров, которые будут контролироваться данной задачей.

  Нажмите кнопку **Редактировать**, чтобы настроить список, тип которого выбран в поле **Компьютеры**.

  Поддерживаются два типа списков компьютеров:

  1. **Статический список** - Все компьютеры задаются в списке по именам и/или IP-адресам. Поскольку этот список статический, то даже если какой-либо компьютер больше не существует в сети, он будет контролироваться задачей, пока запись о нем не будет вручную удалена из этого списка.



  Контролируемые компьютеры задаются в правом списке. Выберите необходимые компьютеры в левом списке и затем переместите их в правый список, нажав кнопку >.

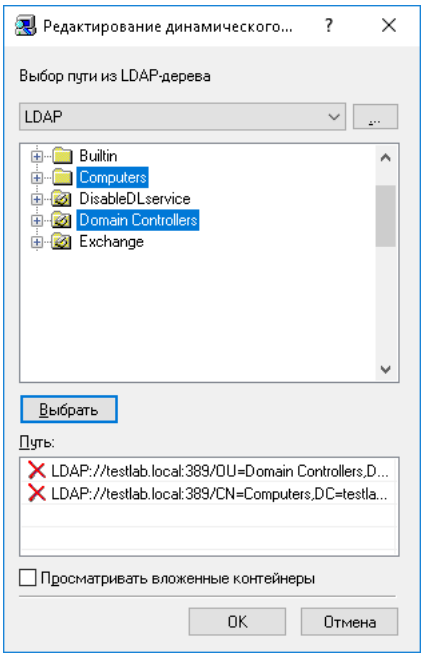
  Если необходимо исключить некоторые компьютеры из процесса мониторинга, то выделите их в правом списке и нажмите кнопку <.

  Используя кнопки >> и <<, можно добавлять и удалять все доступные компьютеры за один раз (не нужно по отдельности выделять компьютеры в списках).

  Имеется несколько вариантов выбора компьютеров в левом списке:

  - **Active Directory** - Просмотреть и выбрать компьютеры из подразделений службы каталогов Active Directory.
  - **Компьютеры** - Просмотреть и выбрать компьютеры из дерева сети.
  - **LDAP** - Просмотреть и выбрать компьютеры из дерева LDAP-совместимой службы каталогов.
  - **Из файла** - Загрузить заранее подготовленный список компьютеров из внешнего текстового файла, а затем выбрать компьютеры. Чтобы открыть внешний файл, нажмите кнопку ... . Текстовый файл может содержать имена компьютеров и/или IP-адреса, каждый из которых должен быть записан на отдельной строке.
  - **Вручную** - Ввести имена компьютеров вручную и затем выбирать компьютеры из полученного списка. Каждое имена или IP-адрес компьютера необходимо вводить на отдельной строке.

2. **Динамический список** - Вместо имен компьютеров или IP-адресов, динамический список содержит путь к контейнеру (например, к подразделению) в дереве службы каталогов (такой как Active Directory, Novell eDirectory, OpenLDAP и т.п.). Каждый раз в момент выполнения задачи DeviceLock Enterprise Server получает все компьютеры, которые в настоящий момент времени существуют в контейнере. Таким образом, если некоторый компьютер был удален из службы каталогов или был перемещен в другой контейнер, то он не будет более контролироваться задачей. И наоборот, если появился новый компьютер, который не существовал в контейнере на момент создания/редактирования задачи, а был добавлен туда позже, то этот новый компьютер будет контролироваться в момент выполнения задачи. Можно выбрать один или несколько контейнеров.



Путь к выбранным контейнерам указывается в поле **Путь**. Выберите контейнеры в дереве щелчком мыши, удерживая нажатой клавишу Shift или Ctrl. Затем нажмите кнопку **Выбрать**. Чтобы отменить выбор контейнера, нажмите красный крестик в поле **Путь**.

Установите флажок **Просматривать вложенные контейнеры**, чтобы разрешить задаче получать компьютеры из всех вложенных контейнеров, находящихся внутри выбранного контейнера. Если этот флажок снят, то все вложенные контейнеры игнорируются и компьютеры получаются только непосредственно из выбранного контейнера.

Предусмотрены два режима работы со службой каталогов:

- **Active Directory** - Просмотр и выбор контейнера из дерева службы каталогов Active Directory.

  Хотя дерево Active Directory может отображаться и в режиме LDAP (см. ниже), мы рекомендуем использовать этот специальный режим Active Directory, т.к. в этом случае DeviceLock Enterprise Server работает со службой каталогов более эффективно и потребляет меньше ресурсов.

Если для доступа к Active Directory вам требуется задать данные альтернативной учетной записи (имя пользователя и пароль), нажмите кнопку ... и укажите в открывшемся диалоговом окне **Параметры доступа** необходимое имя пользователя и соответствующий ему пароль.

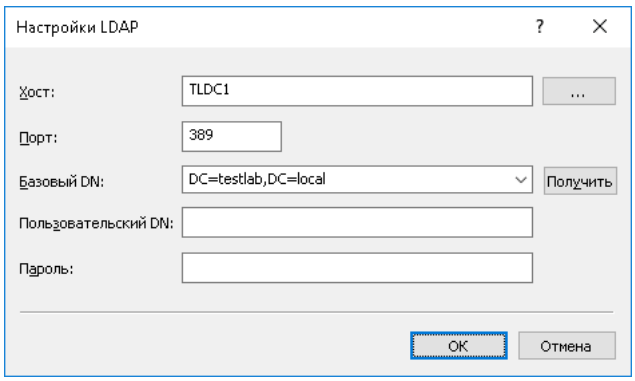
Примечание: Если альтернативная учетная запись не задана, то для доступа к Active Directory используется учетная запись, от имени которой запущена служба DeviceLock Enterprise Server. Дополнительную информацию см. в описании параметра Входить в систему как.

Установите флажок **Синхронизация**, чтобы разрешить серверу DeviceLock Enterprise Server использовать внутренний механизм синхронизации, предоставляемый Active Directory. Использование данного механизма позволяет значительно снизить нагрузку на контроллер домена и быстрее получать компьютеры в момент выполнения задачи.

Примечание: Чтобы использовать механизм синхронизации, требуется доступ к Active Directory с правами администратора.

- **LDAP** - Просмотр и выбор контейнера из дерева LDAP-совместимой службы каталогов.

  Чтобы настроить подключение к LDAP-серверу, нажмите кнопку ... и задайте следующие параметры в диалоговом окне **Настройки LDAP**.



  - **Хост** - Имя или IP-адрес LDAP-сервера, к которому выполняется подключение.
  - **Порт** - Номер порта, по которому LDAP-сервер принимает подключения. По умолчанию это порт 389.
  - **Базовый DN** - Начальная точка для просмотра дерева каталога. Вы должны использовать строку в LDAP-формате (например, cn=qa,o=SMARTLINE,c=US). Оставьте это поле пустым для просмотра с корня дерева.

    Получить все доступные контексты можно, нажав кнопку **Получить**.
  - **Пользовательский DN** - Имя пользователя, под которым выполняется подключение к каталогу. Вы должны использовать строку в LDAP-формате (например, cn=admin,o=SMARTLINE,c=US).

    Примечание: Если имя пользователя не задано, то для доступа к LDAP-серверу используется учетная запись, от имени которой запущена служба DeviceLock Enterprise Server. Дополнительную информацию см. в описании параметра Входить в систему как.
  - **Пароль** - Пароль пользователя.

- **Способы сетевого опроса** - Различные методы сетевого сканирования, используемые для определения статусов (**доступен** или **недоступен**) проверяемых компьютеров.

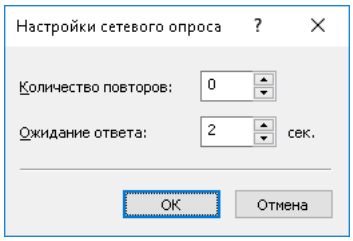
  В момент выполнения задачи сервер DeviceLock Enterprise Server использует все выбранные методы сканирования в перечисленном порядке, пока один из них не вернет статус **доступен** для компьютера. Если ни один из методов не вернул статус **доступен**, то данный компьютер получает статус **недоступен**.

  Поддерживается три метода сетевого сканирования:

  - **Ping-пакеты** - Сервер посылает обычный ICMP-пакет ("пинг") к компьютеру и ждет от него ответа.
  - **NetBIOS-запросы** - Если компонент "Клиент для сетей Microsoft" установлен на компьютере, то этот компьютер ответит на NetBIOS-запрос, отправленный сервером.
  - **Опрос TCP-портов** - Сервер проверяет перечисленные TCP-порты на компьютере и ищет первый открытый порт. Используя запятую (,) или точку с запятой (;) в качестве разделителя, вы можете указать несколько портов одновременно.

    Примечание: Если на компьютере используется какой-либо файрвол, то он может блокировать отсылку некоторых или всех сетевых пакетов. В таком случае данный компьютер получит статус недоступен, даже если он на самом деле включен и работает.

  Чтобы задать дополнительные параметры сканирования, нажмите кнопку **Дополнительные настройки** и задайте следующие параметры в диалоговом окне **Настройки сетевого опроса**.



  - **Количество повторов** - Определяет, какое количество раз DeviceLock Enterprise Server будет повторно выполнять каждый метод сканирования, когда он возвращает статус **недоступен**. Ноль (0) в этом поле означает, что повторных попыток сканирования этим же методом предприниматься не будет (для данного компьютера в данный момент выполнения задачи).
  - **Ожидание ответа** - Время в секундах, в течение которого DeviceLock Enterprise Server ожидает ответ от компьютера для каждого метода сканирования. Если DeviceLock Enterprise Server работает в медленной или чрезмерно загруженной сети, возможно потребуется увеличить это значение.

- **Настройки соединения сервиса** - Эти параметры определяют как DeviceLock Enterprise Server должен подключаться к сервису DeviceLock на контролируемых компьютерах для получения номера версии, настроек и т.п. Если параметры соединения заданы неправильно, то DeviceLock Enterprise Server не сможет подключиться к сервису DeviceLock, и компьютеры, на которых он работает, получат статус **Сервис недоступен**.

  Сервис DeviceLock может быть настроен на использование фиксированного порта или динамических портов в момент установки на компьютер. Дополнительную информацию см. в разделах Установка без вмешательства пользователя и Установка в DeviceLock Enterprise Manager.

Предусмотрены два способа подключения:

- **Динамическая привязка к портам** - Выберите эту опцию для использования сервером DeviceLock Enterprise Server динамических портов при подключении к сервису DeviceLock.
- **Фиксированный TCP-порт** - Если сервис DeviceLock настроен на использование фиксированного TCP-порта, то следует выбрать эту опцию и указать номер порта.

Примечание: Чтобы успешно подключаться к сервису DeviceLock и получать от него необходимую информацию, DeviceLock Enterprise Server должен обладать как минимум правом доступа на чтение на этом сервисе. Если данная задача также должна перезаписывать настройки (политики) на контролируемых экземплярах сервиса, то DeviceLock Enterprise Server должен обладать правом полного доступа к этим экземплярам сервиса.

Для подключения к сервису DeviceLock сервер DeviceLock Enterprise Server использует учетные данные, с которыми были запущена его служба. Если указан секретный ключ, сервер также может использовать аутентификацию на основе сертификата DeviceLock. За дополнительной информацией обращайтесь к описанию параметров Входить в систему как и Имя сертификата.

- **Проверять настройки сервиса** - Установите этот флажок, если требуется, чтобы данная задача мониторинга выполняла проверку настроек сервиса DeviceLock путем их сравнения с определенными эталонными настройками.

  Если данный флажок установлен, то на каждом контролируемом компьютере задача мониторинга проверяет настройки сервиса DeviceLock, сравнивая их с эталонными. При обнаружении настроек, отличающихся от эталонных, компьютеру присваивается статус "Настройки повреждены". Кроме того, событие "Настройки повреждены" регистрируется в журнале мониторинга. Список настроек, отличающихся от эталонных, содержится в записи о событии. Его можно просмотреть при помощи команды **Просмотр деталей** на событии "Настройки повреждены" в журнале мониторинга (см. Просмотрщик журнала мониторинга). Еще один способ просмотра настроек, не совпадающих с эталонными, - использовать команду **Просмотр деталей** на контролируемом компьютере с статусом "Настройки повреждены" (подробнее об этом см. в разделе Задача и ее контролируемые компьютеры).

  - **Файл с настройками сервиса** - Путь и имя файла настроек сервиса DeviceLock, которые считаются эталонной политикой. Для выбора файла служит кнопка рядом с этим полем.

    Эталонная политика назначается задаче путем загрузки определенного файла настроек сервиса DeviceLock. Этот файл можно создать в консоли DeviceLock Service Settings Editor, DeviceLock Management Console или DeviceLock Group Policy Manager.

    В ходе проверки задача получает настройки с контролируемых компьютеров и сравнивает их с файлом настроек, назначенным в качестве эталонной политики для этой задачи.

    Все настройки, не определенные в эталонной политике (параметры, находящиеся в состоянии "не определен"), при проверке не учитываются. Эта функция может использоваться для выборочной проверки интересующих параметров, позволяя другим параметрам отличаться от эталонной политики.

    Для загрузки файла нажмите кнопку ... . Поскольку цифровая подпись на данном этапе не проверяется, можно выбрать подписанный или неподписанный файл. Имя и путь выбранного файла отображается в поле **Файл с настройками сервиса**. В случае подписанного файла его имя и путь заключается в круглые скобки.

    При редактировании задачи, которой уже назначена эталонная политика, параметры эталонной политики можно экспортировать в файл, нажав кнопку **Сохранить**.

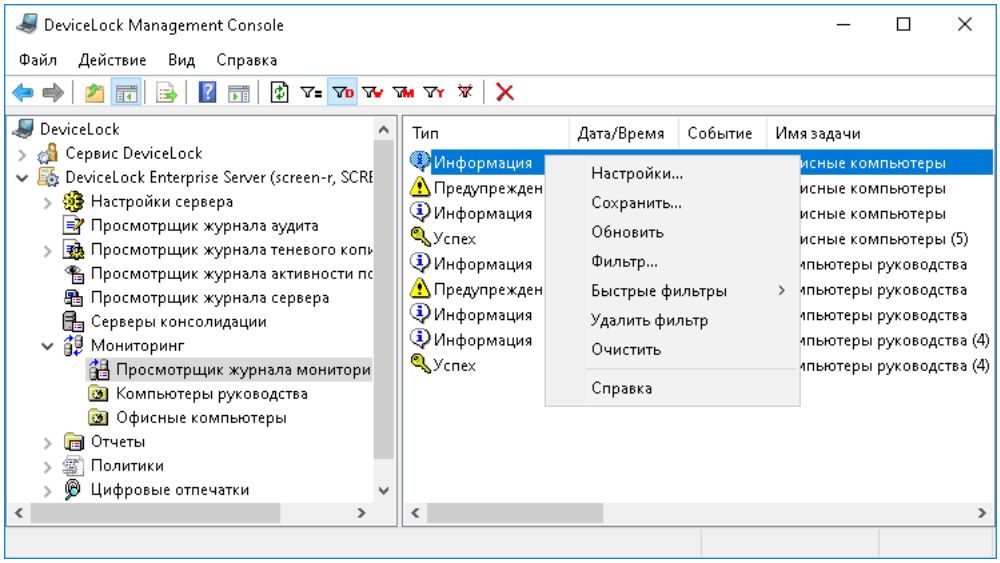
- **Восстанавливать настройки сервиса** - Установите этот флажок, если требуется, чтобы задача мониторинга заменяла поврежденные настройки на контролируемых компьютерах настройками из эталонной политики. Задача, у которой данный флажок установлен, не только проверяет, но и восстанавливает настройки сервиса DeviceLock в случае их изменения или повреждения.

- **Интервал сканирования** - Время в секундах, которое должно пройти после окончания выполнения задачи и перед началом выполнения этой же задачи снова.
- **Количество сканирующих потоков** - Максимальное количество потоков, которое может быть задействовано данной задачей в процессе своего выполнения. Вы можете увеличить это значение, чтобы распараллелить процесс сканирования компьютеров. Тем не менее, большее число потоков требует большего количества ресурсов (особенного памяти и сетевого трафика) для сервера DeviceLock Enterprise Server.
- **Автоматически устанавливать/обновлять Сервис DeviceLock** - Установите этот флажок для автоматической установки сервиса DeviceLock на компьютеры, включенные в задачу мониторинга.
- **Автоматически удалять Сервис DeviceLock** - Установите этот флажок для автоматического удаления сервиса DeviceLock с компьютеров, включенных в задачу мониторинга.

Примечание: Если служба сервера DeviceLock Enterprise Server запускается под локальной учетной записью системы (Local System), то задачи мониторинга не смогут устанавливать, обновлять и удалять сервис DeviceLock на удаленных компьютерах.

Просмотрщик журнала мониторинга

Этот раздел консоли служит для просмотра записей из журнала мониторинга, в котором задачи мониторинга регистрируют информацию о контролируемых ими компьютерах и сервисе DeviceLock на этих компьютерах.



Столбцы просмотрщика определены следующим образом:

- **Тип** - Возможны события следующих типов:
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- **Дата/Время** - Дата и время события.
- **Событие** - Идентификационный номер события.
- **Имя задачи** - Имя задачи мониторинга, вызвавшей событие. Может быть пустым, если событие не имеет отношения к какой-либо задаче мониторинга.
- **Имя компьютера** - Имя компьютера, вызвавшего событие в процессе мониторинга. Может быть пустым, если событие не имеет отношения к мониторингу какого-либо компьютера.
- **Информация** - Описание события, в том числе описание действий и ошибок.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, который зарегистрировал данное событие.
- **Запись N** - Порядковый номер записи в списке событий.
- **Сервер консолидации** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов (см. Консолидация журналов).
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов (см. Консолидация журналов).

Управление журналом мониторинга

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узлы **DeviceLock Enterprise Server** > **Мониторинг** и щелкните правой кнопкой мыши **Просмотрщик журнала мониторинга**.

  - или -

- В дереве консоли DeviceLock Management Console выберите **DeviceLock Enterprise Server** > **Мониторинг** > **Просмотрщик журнала мониторинга** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды:

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале (см. Настройки журнала мониторинга).
- **Сохранить** - Сохранить журнал в указанный файл.
- **Обновить** - Обновить список событий с учетом последних изменений.
- **Просмотр деталей** - На записи о событии "Настройки повреждены" позволяет просмотреть настройки сервиса DeviceLock на контролируемом компьютере, которые отличаются от эталонной политики, заданной в задаче мониторинга (см. описание параметра Проверять настройки сервиса).

  Команда **Просмотр деталей** отображает диалоговое окно со списком настроек, не соответствующих эталонной политике. Каждая такая настройка сопровождается описанием несоответствия, например:

  - **отсутствует** - Настройка задана в эталонной политике, но отсутствует на контролируемом компьютере.
  - **отличается** - Настройка задана по-разному в эталонной политике и на контролируемом компьютере.
  - **избыточно** - Настройка отмечена как удаленная в эталонной политике, но задана на контролируемом компьютере.

- **Фильтр** - Отображать только записи о событиях, которые удовлетворяют заданным условиям (см. Фильтр журнала мониторинга).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра записей за определенный промежуток времени:

  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

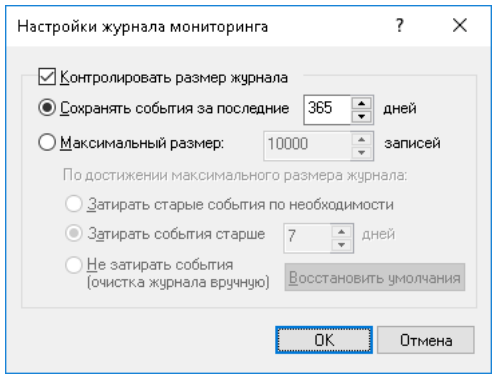
  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).

- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи о событиях, имеющиеся в журнале на данный момент.

Настройки журнала мониторинга

Чтобы контролировать размер журнала и действия сервера при переполнении журнала, выберите команду **Настройки** в контекстном меню просмотрщика этого журнала в дереве консоли. Затем просмотрите или измените настройки в появившемся диалоговом окне.

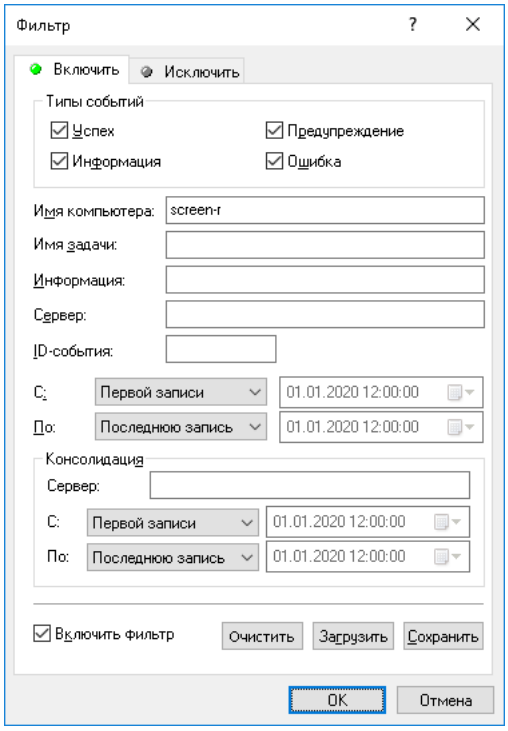


Настройки данного журнала аналогичны настройкам журнала аудита, см. Настройки журнала аудита (для сервера).

Примечание: Сервер удаляет старые записи по дате, указанной в столбце **Дата/Время** (если запись была выполнена локальным сервером), либо по дате, указанной в столбце **Дата/Время консолидации** (если запись была получена от другого сервера посредством консолидации).

Фильтр журнала мониторинга

Просмотрщик журнала мониторинга позволяет применить фильтр для отображения только таких записей, которые удовлетворяют заданным условиям. Чтобы просмотреть или изменить эти условия, выберите команду контекстного меню **Фильтр** или нажмите кнопку ▽ на панели инструментов, а затем используйте появившееся диалоговое окно.



Фильтр журнала мониторинга настраивается аналогично фильтру журнала аудита, описанному в разделе Фильтр журнала аудита (для сервера).

Предусмотрены два типа фильтра:

- **Включить** - Отображать только записи о событиях, которые соответствуют заданным условиям. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Включить** и задайте условия на этой вкладке.
- **Исключить** - Не отображать записи о событиях, которые соответствуют заданным условиям. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Исключить** и задайте условия на этой вкладке.

Фильтр можно временно выключить. Для этого снимите флажок **Включить фильтр**.

Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

Когда фильтр включен, можно задать условия фильтрации, задав необходимые значения в следующих полях:

- **Типы событий** - Фильтрация по типу событий. Возможны следующие варианты (установите соответствующие флажки):
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- Строковые поля, предназначенные для включения или исключения из списка записей о событиях, у которых в указанном поле данных встречается заданная строка. Например, для фильтрации записей по имени задачи, вызвавшей событие, задайте строку фильтра в поле **Имя задачи**. Для фильтрации записей о событиях с определенными ID-номерами, введите номера искомых событий в поле **ID-события**, разделяя их точкой с запятой.

  Предусмотрены следующие строковые поля:

  - **Имя компьютера** - Имя компьютера, вызвавшего событие в процессе мониторинга.
  - **Имя задачи** - Имя задачи мониторинга, вызвавшей событие.
  - **Информация** - Описание события, в том числе описание действий и ошибок.
  - **Сервер** - Имя сервера DeviceLock Enterprise Server, зарегистрировавшего событие.
  - **ID-события** - Идентификационный номер события.

  Примечание: Чтобы облегчить настройку фильтра, его строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

- **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были зарегистрированы сервером.
- **Консолидация** - Поля для фильтрации по данным, относящимся к консолидации журналов (см. Консолидация журналов):
  - **Сервер** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов. Это поле нечувствительно к регистру и позволяет использовать знаки подстановки (* и ?). Используя точку с запятой в качестве разделителя, можно задать несколько значений.
  - **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были последний раз получены с удаленного сервера при консолидации журналов.

Для каждого временного диапазона предусмотрены следующие настройки:

- **С** - Начало диапазона. Возможные значения:
  - **Первой записи** - Фильтровать события, начиная с самой ранней даты и времени в соответствующем поле журнала.
  - **Записи от** - Фильтровать события, начиная с определенной даты и времени.
- **По** - Конец диапазона. Возможные значения:
  - **Последнюю запись** - Фильтровать события, заканчивая самой поздней датой и временем в соответствующем поле журнала.
  - **Записи от** - Фильтровать события, заканчивая определенной датой и временем.

Примечание: Чтобы облегчить настройку фильтра, его строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

12

Политики DeviceLock Enterprise Server

В этой главе:

Общая информация

Сценарии применения политик: пошаговое конфигурирование

Управление политиками DeviceLock

Общая информация

DeviceLock Enterprise Server позволяет автоматически распространять политики безопасности DeviceLock на клиентские компьютеры в сети организации. Если заданы политики получения настроек с сервера DeviceLock Enterprise Server, экземпляры сервиса DeviceLock будут инициировать подключения к серверам DeviceLock Enterprise Server для запроса и получения политик безопасности, что устраняет необходимость проверки, работают ли клиентские компьютеры. Такой подход значительно упрощает и оптимизирует управление политиками безопасности, особенно в средах без Active Directory или как альтернатива использованию групповых политик домена Active Directory.

Для диагностики проблем выполнения политик DeviceLock следует использовать журнал политик. События в данном журнале создаются в ходе применения политики.

Конфигурация политики основана на файле, определяющем настройки сервиса DeviceLock (.dls файл). Создать такой файл можно с помощью консоли DeviceLock Management Console, подключенной к отдельному контролируемому компьютеру; однако лучше использовать для этой цели консоль DeviceLock Service Settings Editor.

Как обрабатываются и применяются политики

Политики могут использоваться для задания конфигурации сервиса DeviceLock на множестве рабочих станций. Сами политики представляют собой набор объектов политики. Каждый объект политики включает четыре (4) основных элемента: имя, список компьютеров, для которых применяется данный объект политики, настройки, заданные в файле настроек сервиса DeviceLock (.dls), и уровень приоритета, используемый для исключения конфликтов при задании различных объектов политики. Если выявлен конфликт двух объектов политики, применяются настройки объекта политики, имеющего больший уровень приоритета. Уровень приоритета может иметь значение от 0 до 100, где 0 является наименьшим уровнем приоритета, а 100 - наибольшим. Если для клиентского компьютера задано 2 или более политики с одинаковым уровнем приоритета, будет применена первая политика, полученная сервисом DeviceLock от сервера.

Можно создавать собственные объекты политик или использовать объект **Политика по умолчанию**, встроенный в DeviceLock Enterprise Server. Объект **Политика по умолчанию** может автоматически применяться ко всем клиентским компьютерам независимо от наличия других объектов политики. Объект **Политика по умолчанию** нельзя удалить, но можно заблокировать наследование данного объекта, что предотвратит его применение. Допускается также частичная модификация объекта **Политика по умолчанию** - например, возможно загрузить настройки из файла шаблона настроек сервиса DeviceLock или изменить статический список клиентских компьютеров, на которых будет применена политика. Изменение имени

объекта (**Политика по умолчанию**) и уровня приоритета не допускаются. Объект **Политика по умолчанию** всегда имеет наименьший уровень приоритета. В случае применения на клиентском компьютере нескольких объектов политики, результирующая политика будет являться суммой всех настроек применяемых объектов политики. В случае выявления конфликта заданных настроек в объектах политик, пользовательские политики будут иметь приоритет над объектом **Политика по умолчанию**.

После того, как настройки заданы в объектах политик, они могут быть применены. Взаимодействие клиент/сервер работает следующим образом:

- Клиентский компьютер находит заданный сервер и направляет запрос на получение политики на сервер для инициации соединения. Запрос политики содержит контрольную сумму текущей политики на клиенте.

  Запрос политики с клиентского компьютера отправляется каждый час либо при наступлении одного из следующих событий:

  - Пользователь включает или перезагружает компьютер, на котором установлен сервис DeviceLock.
  - Пользователь входит в систему.
  - Пользователь щелкает правой кнопкой мыши на значке DeviceLock в области уведомлений панели задач, а затем выбирает команду **Обновить текущее состояние**.

    Значок DeviceLock отображается в области уведомлений, если в настройках сервиса включен параметр Всегда отображать значок в системной области.
  - Сервис DeviceLock переключается из автономного режима (офлайн-профиль) в оперативный режим (обычный профиль).

  Примечание: Политики могут быть получены сервисом DeviceLock только с серверов DeviceLock Enterprise Server, назначенных учетной записи **Все** (Everyone). Серверы, назначенные определенным учетным записям пользователей, не могут быть использованы для распространения политик, но могут быть использованы для сбора журналов событийного протоколирования (аудита) и теневых копий.

- Сервер определяет, какие объекты политик должны быть применены на клиентском компьютере, создает результирующую политику для сервиса DeviceLock посредством слияния настроек из объектов политик, и затем сравнивает контрольные суммы полученной и результирующей политик. Если контрольные суммы различаются, сервер передает результирующую политику на клиентский компьютер. Если политики идентичны, ничего не передается.

  Примечание:
  - Если задан список серверов DeviceLock Enterprise Server, к которым может подключаться сервис DeviceLock, и подключение к первому серверу в списке заданных оказалось не успешным, сервис выбирает следующий сервер в списке для запроса политик.
  - Если клиентский компьютер использует установленный сертификат DeviceLock (открытый ключ), выбранный для подключения сервер должен иметь соответствующий закрытый ключ сертификата. В противном случае передача политик будет невозможна.

Сценарии применения политик: пошаговое конфигурирование

Предусмотрено два основных сценария для распространения политик на клиентские компьютеры через DeviceLock Enterprise Server. Эти сценарии описывают необходимые шаги для успешного применения политик.

Сценарий применения политик 1

В данном сценарии предварительно сконфигурированный сервис DeviceLock, установленный на клиентском компьютере, подключается к заданному серверу DeviceLock Enterprise Server и получает политику для применения. Для использования данного сценария необходимо задать следующие параметры сервиса DeviceLock:

- **DeviceLock Enterprise Server(ы)** - Задает список серверов, к которым может подключаться сервис DeviceLock.
- **Источники политик** - Задает режим применения политик сервисом DeviceLock.

Ниже приведены инструкции для задания соответствующих параметров.

Задание списка серверов DeviceLock Enterprise Server

1. Если используется консоль управления Management Console, выполните следующие действия:

   a) Запустите консоль DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor (самостоятельно или как оснастка консоли DeviceLock Enterprise Manager), выполните следующие действия:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующие действия:

   a) Откройте редактор групповых политик Group Policy Object Editor.

   b) В дереве консоли раскройте **Конфигурация компьютера**, затем раскройте узел **DeviceLock**.

2. Выберите узел **Настройки сервиса**.

   Если в дереве консоли выбрать узел "Настройки сервиса", на панели сведений отобразятся параметры сервиса DeviceLock.

3. На панели сведений выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши параметр **DeviceLock Enterprise Server(ы)**, затем выберите команду **Свойства**.

     - или -

   - Дважды щелкните параметр **DeviceLock Enterprise Server(ы)**.

   Появится диалоговое окно "DeviceLock Enterprise Server(ы)".

4. В списке **DeviceLock Enterprise Server(ы)** дважды щелкните в поле **Серверы** рядом с учетной записью **Все** (Everyone), и введите в это поле имя или IP-адрес компьютера, на котором установлен сервер DeviceLock Enterprise Server.

   Если таких компьютеров несколько, используйте точку с запятой (;) в качестве разделителя компьютерных имен или IP-адресов.

   Политики могут быть получены только с серверов, связанных с учетной записью "Все".

   Для внесения изменений в поле **Серверы** дважды щелкните в этом поле (можно также щелкнуть кнопку **Изменить** или нажать клавишу F2).

   Примечание: Убедитесь, что сервер DeviceLock Enterprise Server установлен надлежащим образом и доступен для компьютеров, на которых установлен сервис DeviceLock.

5. Нажмите кнопку **OK**.

Задание значения параметра "Источники политик"

1. Если используется консоль управления Management Console, выполните следующие действия:

   a) Запустите консоль DeviceLock Management Console и подключитесь к компьютеру, на котором запущен сервис DeviceLock.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Service Settings Editor (самостоятельно или как оснастка консоли DeviceLock Enterprise Manager), выполните следующие действия:

   a) Откройте DeviceLock Service Settings Editor.

   b) В дереве консоли раскройте узел **Сервис DeviceLock**.

   Если используется консоль DeviceLock Group Policy Manager, выполните следующие действия:

   a) Откройте редактор групповых политик Group Policy Object Editor.

   b) В дереве консоли раскройте **Конфигурация компьютера**, затем раскройте узел **DeviceLock**.

2. Выберите узел **Настройки сервиса**.

   Если в дереве консоли выбрать узел "Настройки сервиса", на панели сведений отобразятся параметры сервиса DeviceLock.

3. На панели сведений выполните одно из следующих действий:

   - Щелкните правой кнопкой мыши параметр **Источники политик**, затем выберите команду **Свойства**.

     - или -

   - Дважды щелкните параметр **Источники политик**.

   Появится диалоговое окно "Источники политик".

4. В диалоговом окне **Источники политик** выберите любое из следующих возможных значений данного параметра:
    - **Локальная и групповая** - Если выбрано данное значение, сервис DeviceLock будет применять групповые политики домена или локальную политику компьютера, при этом политики сервера DeviceLock Enterprise Server будут игнорироваться.
    - **Локальная и Enterprise Server** - Если выбрано данное значение, сервис DeviceLock будет применять политики сервера DeviceLock Enterprise Server или локальную политику компьютера, при этом групповые политики домена будут игнорироваться.
5. Нажмите кнопку **OK**.

После того, как заданы эти настройки, можно настроить сервер DeviceLock Enterprise Server для распространения политик на компьютеры, где работает сервис DeviceLock. Для получения подробной информации см. раздел Управление политиками DeviceLock.

Сценарий применения политик 2

В данном сценарии ранее установленный сервис DeviceLock обновляется до более новой версии (с поддержкой политик сервера DeviceLock Enterprise Server) и может получать политики по требованию сервера. Для использования данного сценария необходимо выполнение следующего условия:

- Параметр **Источники политик** сервиса DeviceLock должен быть не задан, или установлен в значение **Локальная и Enterprise Server**.

Для получения подробной информации о том, как задать значение параметра **Источники политик**, см. инструкцию Задание значения параметра “Источники политик” выше в данной главе.

Подробное описание процедуры установки режима получения политик по требованию сервера см. в разделе Немедленное применение политик к клиентским компьютерам ниже в данной главе.

Управление политиками DeviceLock

Управление политиками DeviceLock предполагает:

- Использование узла “Политики”
- Управление объектами политики
- Управление компьютерами, назначенными объектам политики
- Просмотр журнала политик

Использование узла “Политики”

DeviceLock Enterprise Server позволяет автоматически распространять политики безопасности DeviceLock на клиентские компьютеры в сети организации. Если заданы политики получения настроек от DeviceLock Enterprise, сервис DeviceLock на клиентских компьютерах будет инициировать подключение к серверам DeviceLock Enterprise Server для запроса и получения политик безопасности, что устраняет необходимость проверки, работают ли клиентские компьютеры. Такой подход значительно упрощает и оптимизирует управление политиками безопасности, особенно в средах без Active Directory или как альтернатива использованию групповых политик домена Active Directory.

Политики сервера DeviceLock Enterprise Server представляют собой набор объектов политики. Каждый объект политики включает четыре основных элемента: имя; список компьютеров, для которых применяется данный объект политики; настройки, заданные в файле настроек сервиса DeviceLock (файл .dls); и уровень приоритета, используемый для исключения конфликтов при задании различных объектов политики. Все объекты политики, которые в данный момент имеются на сервере, отображаются в узле консоли **DeviceLock Enterprise Server** > **Политики**.

Выбрав узел **Политики** в дереве консоли, на панели сведений можно увидеть список всех объектов политики, имеющихся на сервере в данный момент. Панель сведений отображает список со следующими сведениями по каждому объекту политики:

- **Имя объекта политики** - Имя, идентифицирующее объект политики.
- **Время последнего обновления** - Дата и время последнего изменения данного объекта политики.
- **Файл настроек** - Имя файла настроек сервиса DeviceLock (.dls файл), задающего настройки сервиса DeviceLock в данном объекте политики.
- **Автор** - Учетная запись пользователя, создавшего данный объект политики.
- **Приоритет** - Уровень приоритета данного объекта политики. Большее число означает более высокий приоритет.
- **ID-объекта политики** - Уникальный численный идентификатор объекта политики.

Контекстное меню узла **Политики** содержит следующую команду:

- **Создать объект политики** - Создать новый объект политики. Параметры нового объекта политики можно задать в диалоговом окне, которое открывает эта команда. Подробнее см. в разделе Создание пользовательского объекта политики.

Контекстное меню объекта политики на панели сведений содержит следующие команды:

- **Редактировать объект политики** - Просмотреть или изменить параметры объекта политики в диалоговом окне, которое открывает эта команда.
- **Редактировать список компьютеров** - Просмотреть или изменить список компьютеров, назначенных данному объекту политики. Список компьютеров можно редактировать в диалоговом окне, которое открывает эта команда.
- **Загрузить политику** - Загрузить или заменить файл настроек сервиса DeviceLock (файл .dls) в данном объекте политики. Требуемый файл настроек можно выбрать с помощью диалогового окна, которое открывает эта команда.

  Файлы .dls служат для хранения настроек сервиса DeviceLock. Создать такой файл можно с помощью консоли DeviceLock Management Console, подключенной к компьютеру, на котором запущен сервис DeviceLock; однако лучше использовать для этой цели консоль DeviceLock Service Settings Editor.
- **Сохранить политику** - Сохранить настройки политики в файл настроек сервиса DeviceLock (файл .dls). Файл для сохранения настроек указывается в диалоговом окне, которое открывает эта команда.

  Сохранение настроек политики в файле может быть полезным, если нужно загрузить их в другой объект политики. Для этого можно последовательно использовать команды **Сохранить политику** и **Загрузить политику**.
- **Удалить объект политики** - Удалить выбранный объект политики.
- **Применить сейчас** - Немедленно отправить политики из выбранного объекта на все клиентские компьютеры, назначенные данному объекту политики. Если этим компьютерам назначены также другие объекты политики, будет отправлена результирующая политика.
- **Обновить** - Обновляет список на панели сведений с учетом последних изменений.

  Поскольку информация на панели сведений не обновляется автоматически, для ее обновления следует использовать команду **Обновить**.

Объект политики

Политики сервера DeviceLock Enterprise Server представляют собой набор объектов политики. Каждый объект политики включает четыре основных элемента: имя; список компьютеров, для которых применяется данный объект политики; настройки, заданные в файле настроек сервиса DeviceLock (файл .dls); и уровень приоритета, используемый для исключения конфликтов при задании различных объектов политики.

Объекты политики отображаются в дереве консоли под узлом **DeviceLock Enterprise Server** > **Политики**.

Выбрав объект политики в дереве консоли, можно увидеть список всех компьютеров, для которых применяется данный объект политики. Панель сведений консоли отображает список компьютеров со следующими сведениями по каждому компьютеру:

- **Имя компьютера** - Имя, идентифицирующее компьютер.
- **Статус** - Текущий статус компьютера. Возможные статусы ассоциированы с соответствующими иконками:
    - Иконка: Серый компьютер, статус: **(пусто).** Временный статус, отображаемый сразу после создания объекта политики. Изменяется после первой попытки сервера DeviceLock Enterprise Server установить соединение с сервисом DeviceLock и применить на нем политику.
    - Иконка: Зеленый компьютер, статус: **Компьютер доступен**. Данный статус означает, что компьютер работает и на нем запущен сервис DeviceLock.
    - Иконка: Зеленый компьютер с восклицательным знаком, статус: **Используется групповая политика**. Данный статус означает, что на компьютере применяется групповая политика, а DeviceLock Enterprise Server не может применять серверные политики.
    - Иконка: Зеленый компьютер с восклицательным знаком, статус: **Используется локальная политика**. Данный статус означает, что на компьютере применяется локальная политика, поскольку параметр **Использовать групповые/серверные политики** отключен в настройках сервиса DeviceLock.
    - Иконка: Зеленый компьютер с восклицательным знаком, статус: **Используется политика Acronis Cyber Protect**. Данный статус означает, что сервис DeviceLock использует политику, полученную от системы киберзащиты Acronis, и игнорирует политики из любого другого источника.
    - Иконка: Красный компьютер, статус: **Компьютер недоступен**. Данный статус означает, что DeviceLock Enterprise Server не может установить подключение к сервису DeviceLock на компьютере.
    - Иконка: Красный компьютер с восклицательным знаком, статус: **Невозможно определить адрес компьютера**. Данный статус означает, что DeviceLock Enterprise Server не может определить имя/адрес компьютера.
    - Иконка: Зеленый компьютер с восклицательным знаком, статус: **Неподдерживаемая версия сервиса**. Данный статус означает, что DeviceLock Enterprise Server пытался применить серверные политики к сервису DeviceLock версии 8.1 или более ранней. Применение политик сервера DeviceLock Enterprise Server поддерживается только для версии 8.2 и более поздних. Данный статус также может означать, что версия сервиса DeviceLock выше версии сервера.

- Иконка: Зеленый компьютер с восклицательным знаком, статус: **Доступ запрещен**. Данный статус означает, что DeviceLock Enterprise Server не может установить подключение к сервису DeviceLock на компьютере вследствие отсутствия привилегий. Такая ситуация происходит, когда учетная запись, под которой запущена служба сервера DeviceLock Enterprise Server, не имеет достаточных прав для подключения к сервису DeviceLock. Также возможна ситуация, когда открытый ключ сертификата, установленного на компьютере с сервисом DeviceLock и закрытый ключ сертификата, установленного на компьютере, где работает сервер DeviceLock Enterprise Server, не соответствуют друг другу.
- Иконка: Зеленый компьютер с восклицательным знаком, статус: **Лицензия недоступна**. Данный статус означает, что DeviceLock Enterprise Server не может применить политики на компьютере с запущенным сервисом DeviceLock по причине недостаточного количества лицензий. DeviceLock Enterprise Server работает только с тем количеством компьютеров, которое было лицензировано.
- Иконка: Красный компьютер с восклицательным знаком, статус: **Ошибка**. Данный статус означает, что при выполнении политики на компьютере возникла ошибка, не перечисленная выше в других возможных статусах.

- **Время последнего применения** - Дата и время последнего применения политики в формате `dd.mm.yyyy hh:mm:ss`, например, `20.12.2016 13:55:28`.
- **Время последнего подключения** - Дата и время последнего установления подключения к сервису DeviceLock в формате `dd.mm.yyyy hh:mm:ss`, например, `20.12.2016 13:55:28`.
- **Назначенные объекты политики** - Имена всех объектов политики, назначенных компьютеру. Имена в списке разделяются запятыми и перечисляются в порядке приоритета, от высшего к низшему.
- **Примененные объекты политики** - Имена всех объектов политики, примененных на компьютере. Имена в списке разделяются запятыми и перечисляются в порядке приоритета, от высшего к низшему.
- **Версия сервиса** - Номер версии и номер сборки сервиса DeviceLock.

Контекстное меню объекта политики в дереве консоли содержит те же команды, что меню объекта политики на панели сведений. Описание команд см. в разделе Использование узла “Политики”.

Контекстное меню компьютера на панели сведений содержит следующие команды:

- **Подключиться к сервису DeviceLock** - Подключить консоль DeviceLock Management Console к сервису DeviceLock, запущенному на данном компьютере.
- **Редактировать объект политики** - Просмотреть или изменить параметры объекта политики, выбранного в дереве консоли. Параметры объекта можно редактировать в диалоговом окне, которое открывает эта команда.
- **Редактировать список компьютеров** - Просмотреть или изменить список назначенных компьютеров для объекта политики, выбранного в дереве консоли. Список компьютеров можно редактировать в диалоговом окне, которое открывает эта команда.
- **Назначить объекту политики** - Задать объекты политики для данного компьютера. В списке, отображаемом этой командой, можно устанавливать или снимать флажки, назначая или отменяя объекты политики для данного компьютера.

  Если выбрано несколько компьютеров, команда **Назначить объекту политики** позволяет назначать объекты политики всем выбранным компьютерам. Дополнительная команда **Удалить из объекта политики** позволяет отменять назначение объектов политики для всех выбранных компьютеров.

- **Исключить из всех объектов политики** - Отменяет назначение всех объектов политики для данного компьютера.

  В результате, компьютер будет получать только объект **Политика по умолчанию**, если сервис DeviceLock на этом компьютере настроен на использование политик сервера DeviceLock Enterprise Server.

- **Загрузить политику** - Загрузить или заменить файл настроек сервиса DeviceLock (файл .dls) в данном объекте политики. Требуемый файл настроек можно выбрать с помощью диалогового окна, которое открывает эта команда.

  Файлы .dls служат для хранения настроек сервиса DeviceLock. Создать такой файл можно с помощью консоли DeviceLock Management Console, подключенной к компьютеру, на котором запущен сервис DeviceLock; однако лучше использовать для этой цели консоль DeviceLock Service Settings Editor.

- **Сохранить политику** - Сохранить настройки политики в файл настроек сервиса DeviceLock (файл .dls). Файл для сохранения настроек указывается в диалоговом окне, которое открывает эта команда.

  Сохранение настроек политики в файле может быть полезным, если нужно загрузить их в другой объект политики. Для этого можно последовательно использовать команды **Сохранить политику** и **Загрузить политику**.

- **Удалить объект политики** - Удалить объект политики, выбранный в дереве консоли.

- **Применить сейчас** - Немедленно отправить политики из объекта, выбранного в дереве консоли, на все клиентские компьютеры, назначенные этому объекту политики. Если компьютерам назначены также другие объекты политики, будет отправлена результирующая политика.

- **Обновить** - Обновляет список компьютеров с учетом последних изменений.

  Поскольку информация, отображаемая в списке компьютеров, не обновляется автоматически, для ее обновления следует использовать команду **Обновить**.

Политика по умолчанию

Политика по умолчанию - это встроенный объект сервера DeviceLock Enterprise Server, который может автоматически применяться ко всем клиентским компьютерам независимо от наличия других объектов политики. Подробнее об этом объекте см. в разделе Как обрабатываются и применяются политики.

Допускается также частичная модификация объекта **Политика по умолчанию** - например, возможно загрузить настройки из файла настроек сервиса DeviceLock (.dls) или задать статический список клиентских компьютеров, на которых будет применена политика по умолчанию.

Объект Политика по умолчанию отображается в дереве консоли под узлом **DeviceLock Enterprise Server** > **Политики**.

Контекстное меню объекта **Политика по умолчанию** содержит те же команды, что и меню обычного объекта политики. Описание команд см. в разделе Объект политики.

Если в дереве консоли выбран объект **Политика по умолчанию**, на панели сведений отображается список всех компьютеров, назначенных этому объекту политики. Описание списка компьютеров см. в разделе Объект политики.

Контекстное меню компьютера на панели сведений содержит те же команды, что и в случае выбора обычного объекта политики. Описание команд см. в разделе Объект политики.

Управление объектами политики

Политики DeviceLock определяются объектами политики. Возможно использование собственных (пользовательских) объектов политики или объекта **Политика по умолчанию**, встроенного в сервер DeviceLock Enterprise Server.

Управление объектами политики предполагает:

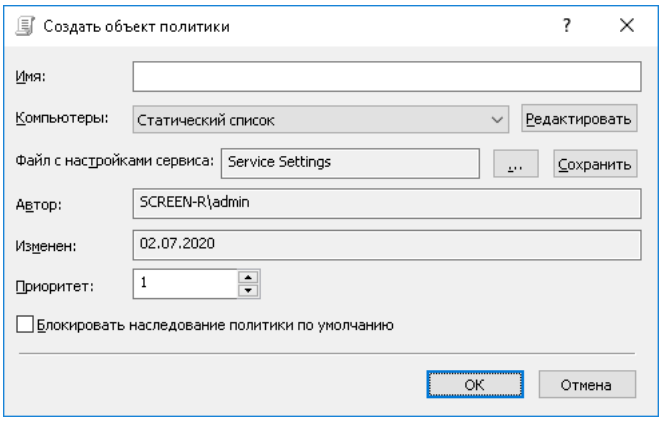
- Создание пользовательского объекта политики
- Редактирование объекта политики
- Удаление пользовательского объекта политики
- Восстановление значений по умолчанию для объекта "Политика по умолчанию"

Создание пользовательского объекта политики

Для создания пользовательского объекта политики

1. Откройте консоль управления DeviceLock Management Console и подключитесь к компьютеру, на котором работает DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** щелкните правой кнопкой мыши узел **Политики**, и выберите команду **Создать объект политики**.

   Появится диалоговое окно "Создать объект политики".



4. В диалоговом окне **Создать объект политики** выполните следующие действия:
   - **Имя** - Задать имя объекта политики.
   - **Компьютеры** - Назначить компьютеры объекту политики. Для этого выберите опцию **Статический список** или **Динамический список**, а затем настройте список компьютеров в соответствии с вашими требованиями.
   - **Статический список** - Данная опция позволяет задать объекту политики статический список компьютеров. Если выбрана данная опция:
     a) Нажмите кнопку **Редактировать**, чтобы открыть диалоговое окно **Редактирование статического списка**.
     b) В диалоговом окне **Редактирование статического списка** выберите компьютеры, используя один из следующих вариантов: **Active Directory**, **Компьютеры**, **LDAP**, **Из файла**, **Вручную**.
        - Опция **Active Directory** позволяет выбрать компьютеры из службы каталогов Active Directory. Нажав кнопку ..., можно задать имя пользователя и пароль для доступа к Active Directory.
        - Опция **Компьютеры** позволяет просматривать и выбирать компьютеры из дерева сети.
        - Опция **LDAP** позволяет выбирать компьютеры из LDAP-совместимой службы каталогов. Нажмите кнопку ..., чтобы задать параметры соединения со службой каталогов.
        - Опция **Из файла** позволяет импортировать список компьютеров из текстового файла с последующим выбором компьютеров.

          Чтобы открыть такой текстовый файл, нажмите кнопку ... Такой текстовый файл должен содержать один компьютер на строку и может быть в кодировке Unicode или non-Unicode.
        - Опция **Вручную** позволяет позволяет ввести имена компьютеров вручную. Каждое имя компьютера или его IP-адрес должно вводиться на отдельной строке.

     Все выбранные компьютеры отображаются в правой части диалогового окна.

     Для удаления отдельных компьютеров из списка используйте кнопку со стрелкой влево < . Для массового единовременного добавления всех доступных имен компьютеров или удаления всех выбранных компьютеров используйте кнопки с двойными стрелками соответственно вправо >> или влево << .

- **Динамический список** - Данная опция позволяет задать динамический список компьютеров, который будет автоматически обновляться по мере их добавления или удаления из определенного контейнера службы каталогов. Если выбрана данная опция:

  a) Нажмите кнопку **Редактировать**, чтобы открыть диалоговое окно **Редактирование динамического списка**.

  b) В диалоговом окне **Редактирование динамического списка** выберите нужный контейнер в дереве AD или LDAP, затем нажмите кнопку **Выбрать**. Можно выбрать один или несколько контейнеров.

     Для включения в динамический список компьютеров из контейнеров уровнем ниже выбранного, установите флаг **Просматривать вложенные контейнеры**.

     Для выполнения синхронизации с Active Directory установите флаг **Синхронизация**.

  Кнопка ... открывает диалоговое окно **Параметры доступа** (если выбрана опция **Active Directory**) или **Настройки LDAP** (если выбрана опция **LDAP**). Диалоговое окно **Параметры доступа** позволяет указать имя и пароль пользователя с административными правами доступа в AD. Диалоговое окно **Настройки LDAP** позволяет задать параметры подключения к серверу LDAP.

- **Файл с настройками сервиса** - Назначить объекту политики настройки сервиса DeviceLock, сохраненные в файле настроек (.dls). Нажмите кнопку ..., чтобы загрузить файл с сохраненными настройками сервиса DeviceLock (файл .dls). При слиянии множества политик не заданные настройки будут проигнорированы. При применении политики на сервисе DeviceLock все не заданные настройки будут сброшены к значениям по умолчанию. Для сохранения текущей назначенной политики в файл нажмите кнопку **Сохранить**.

- **Приоритет** - Задать значение уровня приоритета от 0 до 100, где 0 - наименьший уровень приоритета, а 100 - наивысший. Приоритет политик используется для разрешения конфликтов настроек и параметров в различных объектах политики. При выявлении конфликта параметров в двух или более объектах политики, будут применены настройки объекта политики с наибольшим приоритетом.

- **Блокировать наследование политики по умолчанию** - Запретить применение объекта **Политика по умолчанию** на всех компьютеров, назначенных объекту политики. Если флажок **Блокировать наследование политики по умолчанию** установлен, объект **Политика по умолчанию** не применяется к компьютерам, назначенным данному объекту политики. Снимите этот флажок, чтобы разрешить применение объекта **Политика по умолчанию** к таким компьютерам.

  Примечание: Если какому-либо компьютеру назначено несколько объектов политики, и по крайней мере у одного из них установлен флажок **Блокировать наследование политики по умолчанию**, объект **Политика по умолчанию** не будет применяться на таком компьютере.

5. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Создать объект политики**.

   Созданный объект появится в дереве консоли ниже объекта "Политика по умолчанию".

Редактирование объекта политики

Существующий объект политики может быть изменен для обеспечения точного соответствия текущим задачам.

Для редактирования объекта политики

1. Откройте консоль управления DeviceLock Management Console и подключитесь к компьютеру, на котором запущен DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** раскройте узел **Политики**, затем выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши объект политики, который требуется изменить, затем выберите команду **Редактировать объект политики**.

     - или -
   - Выберите объект политики, который требуется изменить. на панели сведений щелкните правой кнопкой мыши любой компьютер, назначенный объекту политики, а затем выберите команду **Редактировать объект политики**.
4. В появившемся диалоговом окне **Редактировать объект политики** измените настройки по своему усмотрению.
5. Нажмите кнопку **OK** для применения изменений.

Удаление пользовательского объекта политики

Созданные пользователем объекты политики, если они больше не нужны, можно удалять. Объект **Политика по умолчанию** не может быть удален.

Для удаления пользовательского объекта политики

1. Откройте консоль управления DeviceLock Management Console и подключитесь к компьютеру, на котором запущен DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** раскройте узел **Политики**, затем выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши объект политики, который требуется удалить, затем выберите команду **Удалить объект политики**.

     - или -
   - Выберите объект политики, который требуется удалить. на панели сведений щелкните правой кнопкой мыши любой компьютер, назначенный объекту политики, а затем выберите команду **Удалить объект политики**.

Восстановление значений по умолчанию для объекта “Политика по умолчанию”

Для восстановления значений по умолчанию в объекте **Политика по умолчанию** требуется удалить назначенный файл настроек сервиса DeviceLock (.dls) и статический список компьютеров, назначенный данному объекту политики.

Для восстановления значений по умолчанию для объекта “Политика по умолчанию”

1. Откройте консоль управления DeviceLock Management Console и подключитесь к компьютеру, на котором запущен DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** раскройте узел **Политики**.
4. В узле **Политики** щелкните правой кнопкой мыши объект **Политика по умолчанию**, затем выберите команду **Очистить объект политики**.

Управление компьютерами, назначенными объектам политики

Управление компьютерами, назначенными объектам политики, предполагает:

- Немедленное применение политик к клиентским компьютерам
- Изменение объекта политики на клиентском компьютере
- Удаление клиентского компьютера из всех объектов политики
- Обновление списка назначенных компьютеров и информации об исполнении политики

Немедленное применение политик к клиентским компьютерам

Если расписание отправки политики на клиентские компьютеры не соответствует текущим требованиям, можно принудительно отправить политики с сервера DeviceLock Enterprise Server на клиентские компьютеры. Режим принудительной отправки политик с сервера (режим push) также используется в сценарии, где сервис DeviceLock не был настроен для использования политик сервера DeviceLock Enterprise Server. Более подробная информация приведена в разделе Сценарий применения политик 2.

Для немедленной отправки политик на клиентские компьютеры

1. Откройте консоль управления DeviceLock Management Console и подключитесь к компьютеру, на котором запущен DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** раскройте узел **Политики**, затем выполните одно из следующих действий:
   - Щелкните правой кнопкой мыши нужный объект политики, а затем выберите команду **Применить сейчас**.

     Это действие приводит к тому, что DeviceLock Enterprise Server немедленно отправляет политики из выбранного объекта на все клиентские компьютеры, назначенные данному объекту политики. Если этим компьютерам назначены также другие объекты политики, будет отправлена результирующая политика.

     - или -
   - Выберите нужный объект политики в дереве консоли. На панели сведений щелкните правой кнопкой мыши один из компьютеров, назначенных этому объекту политики, а затем выберите команду **Применить сейчас**.

     Это действие приводит к тому, что DeviceLock Enterprise Server немедленно отправляет политики из выбранного объекта на выбранный вами компьютер. Если этому компьютеру назначены также другие объекты политики, будет отправлена результирующая политика.

Изменение объекта политики на клиентском компьютере

Отдельным компьютерам или группе компьютеров может быть переназначен новый объект политики.

Для изменения объекта политики на компьютере

1. Откройте консоль управления DeviceLock Management Console и подключитесь к компьютеру, на котором запущен DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** раскройте узел **Политики**.
4. В узле **Политики** выберите объект политики, назначенный искомому компьютеру.

   Если в дереве консоли выбрать объект политики, на панели сведений отобразятся все компьютеры, назначенные данному объекту политики. Кроме того, отображается информация об исполнении политики для каждого компьютера из этого списка.
5. На панели сведений щелкните правой кнопкой мыши любой компьютер, для которого требуется назначить другой объект политики, выберите команду **Назначить объекту политики**, и затем выберите требуемый объект политики.

   Чтобы выбрать одновременно несколько компьютеров, удерживайте нажатой клавишу SHIFT или CTRL при выборе компьютеров на панели сведений.

Удаление клиентского компьютера из всех объектов политики

При необходимости возможно удалить выбранный клиентский компьютер из всех объектов политики на сервере DeviceLock Enterprise Server. Данная операция также отменяет результаты применения политики.

Примечание: Если на указанном компьютере установлен сервис DeviceLock, настроенный на получение политик с сервера DeviceLock Enterprise Server, то при запросе политики с сервера на такой компьютер будут отправлены настройки из объекта **Политика по умолчанию**.

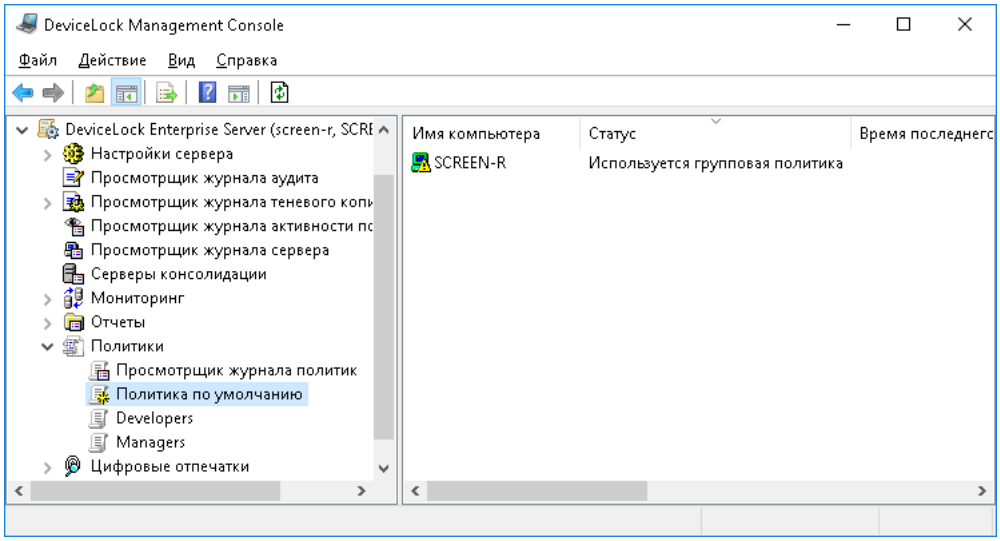
Для удаления клиентского компьютера из всех объектов политики

1. Откройте консоль управления DeviceLock Management Console и подключитесь к компьютеру, на котором запущен DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** раскройте узел **Политики**.
4. В узле **Политики** выберите объект политики, назначенный искомому компьютеру.

   Если в дереве консоли выбрать объект политики, на панели сведений отобразятся все компьютеры, назначенные данному объекту политики. Кроме того, отображается информация об исполнении политики для каждого компьютера из этого списка.
5. На панели сведений щелкните правой кнопкой мыши любой компьютер, который требуется удалить из всех объектов политики, затем выберите команду **Исключить из всех объектов политики**.

Обновление списка назначенных компьютеров и информации об исполнении политики

При выборе объекта политики в дереве консоли панель сведений отображает список всех компьютеров, назначенных данному объекту политики.



В этом списке можно просмотреть информацию о выполнении политики для каждого компьютера. Описание списка компьютеров см. в разделе Объект политики.

Список компьютеров и информация об исполнении политики на панели сведений не обновляются автоматически, для их обновления требуется выполнить следующие действия.

Для обновления списка назначенных компьютеров и информации об исполнении политики

1. Откройте консоль управления DeviceLock Management Console и подключитесь к компьютеру, на котором запущен DeviceLock Enterprise Server.
2. В дереве консоли раскройте узлы **DeviceLock Enterprise Server** > **Политики**.
3. В узле **Политики** щелкните правой кнопкой мыши на любом объекте политики, затем выберите команду **Обновить**.

   - или -

   В узле **Политики** выберите любой объект политики, затем выполните одно из следующих действий:

   - Нажмите кнопку **Обновить** на панели инструментов.

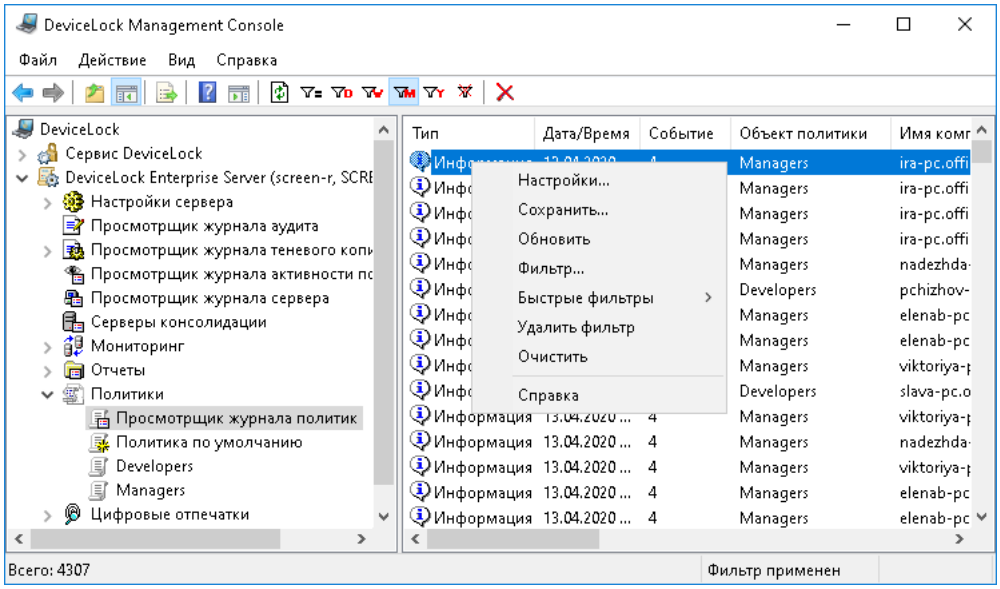
     - или -

   - Щелкните правой кнопкой мыши на панели сведений, затем выберите команду **Обновить**.

   Если в дереве консоли выбрать объект политики, на панели сведений отобразятся все компьютеры, назначенные данному объекту политики. Кроме того, отображается информация об исполнении политики для каждого компьютера из этого списка.

Просмотр журнала политик

События, записанные в журнал политик, помогают выяснять и устранять причины неполадок при администрировании и исполнении политик. Для просмотра журнала выберите **DeviceLock Enterprise Server** > **Политики** > **Просмотрщик журнала политик** в дереве консоли.



Панель сведений консоли отображает список событий, зарегистрированных в журнале политик, со следующей информацией по каждому событию:

- **Тип** - Возможны события следующих типов:
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- **Дата/Время** - Дата и время события.
- **Событие** - Идентификационный номер события.
- **Объект политики** - Имя объекта политики, связанного с событием.
- **Имя компьютера** - Имя компьютера, вызвавшего данное событие.
- **Информация** - Описание события, в том числе описание действий и ошибок.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, который зарегистрировал данное событие.
- **Запись N** - Порядковый номер записи в списке событий.
- **Сервер консолидации** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов (см. Консолидация журналов).
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов (см. Консолидация журналов).

Управление журналом политик

Для управления журналом служат команды контекстного меню:

- В дереве консоли DeviceLock Management Console раскройте узлы **DeviceLock Enterprise Server** > **Политики** и щелкните правой кнопкой мыши **Просмотрщик журнала политик**.

  - или -

- В дереве консоли DeviceLock Management Console выберите **DeviceLock Enterprise Server** > **Политики** > **Просмотрщик журнала политик** и щелкните правой кнопкой мыши какую-либо запись в списке событий на панели сведений.

В контекстном меню предоставляются следующие команды:

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале (см. Настройки журнала политик).
- **Сохранить** - Сохранить журнал в указанный файл.
- **Обновить** - Обновить список событий с учетом последних изменений.
- **Фильтр** - Отображать только записи о событиях, которые удовлетворяют заданным условиям (см. Фильтр журнала политик).
- **Быстрые фильтры** - Выбор одного из следующих вариантов для просмотра записей за определенный промежуток времени:
  - Текущий день
  - Текущая неделя
  - Текущий месяц
  - Текущий год

  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).
- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи о событиях, имеющиеся в журнале на данный момент.

  Эта команда добавляет в журнал запись об удалении, указывающую, сколько записей было удалено, а также кто выполнил удаление и с какого компьютера.

Настройки журнала политик

Чтобы контролировать размер журнала и действия сервера при переполнении журнала, используйте команду Настройки из контекстного меню просмотрщика этого журнала в дереве консоли. Эта команда отображает диалоговое окно со следующими настройками:

- **Контролировать размер журнала** - Установите этот флажок, чтобы позволить серверу контролировать количество записей в журнале и удалять устаревшие записи. Если этот флажок не установлен, сервер использует все доступное пространство базы данных для хранения журнала.
- **Сохранять события за последние** <число> **дней** - Если выбран этот параметр, в журнале хранятся записи не старше заданного количества дней (по умолчанию - 365 дней).
- **Максимальный размер:** <число> **записей** - Если выбран этот параметр, в журнале хранится не более заданного количества записей. В этом случае необходимо выбрать действие сервера, которое будет выполняться, когда журнал достигнет максимального размера:
  - **Затирать старые события по необходимости** - Новые записи событий продолжают сохраняться при достижении максимального размера журнала. Каждая запись нового события заменяет собой самую старую запись в журнале.
  - **Затирать события старше** <число> **дней** - Новые записи событий заменяют собой только записи, хранящиеся дольше заданного количества дней. Поддерживаемая настройка - до 32 767 дней.
  - **Не затирать события (очистка журнала вручную)** - При достижении максимального размера журнала новые записи событий не добавляются. Чтобы обеспечить их добавление, необходимо очистить журнал вручную.

Примечание: Сервер удаляет старые записи по дате, указанной в столбце **Дата/Время** (если запись была выполнена локальным сервером), либо по дате, указанной в столбце **Дата/Время консолидации** (если запись была получена от другого сервера посредством консолидации).

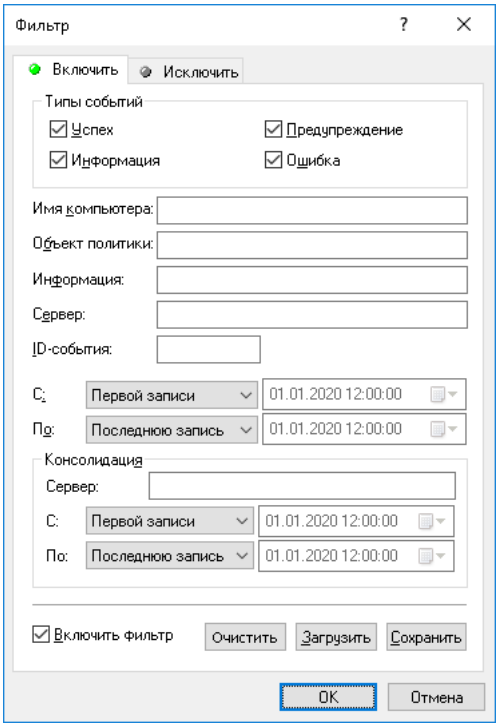
Внимание: Если в журнале нет места для новых записей, а настройки журнала не позволяют удалить старые записи, сервер не будет добавлять новые записи в журнал.

Чтобы использовать настройки по умолчанию, нажмите кнопку **Восстановить умолчания**. В результате будут установлены следующие настройки:

- Максимальный размер: 10 000 записей
- Затирать события старше 7 дней

Фильтр журнала политик

В результате фильтрации список событий отображает только те записи, которые соответствуют условиям фильтрации. Чтобы просмотреть или изменить условия фильтрации, выберите команде **Фильтр** в контекстном меню списка событий или нажмите кнопку ▽= на панели инструментов. Параметры фильтра задаются в диалоговом окне **Фильтр**:



Диалоговое окно **Фильтр** предоставляет следующие параметры для настройки фильтра:

- **Включить** - Консоль отображает только события, удовлетворяющие условиям, заданным на вкладке **Включить**. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Включить**.
- **Исключить** - Консоль не отображает события, удовлетворяющие условиям, заданным на вкладке **Исключить**. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Исключить**.

  Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

- **Типы событий** - Фильтрация по типу событий. Возможны следующие варианты (установите соответствующие флажки):
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Произошла ошибка.
- Строковые поля, предназначенные для включения или исключения из списка записей о событиях, у которых в указанном поле данных встречается заданная строка. Например, для фильтрации записей по имени компьютера, вызвавшего событие, задайте строку фильтра в поле **Имя компьютера**. Для фильтрации записей о событиях с определенными ID-номерами, введите номера искомых событий в поле **ID-события**, разделяя их точкой с запятой.

Предусмотрены следующие строковые поля:

- **Имя компьютера** - Имя компьютера, вызвавшего событие.
- **Объект политики** - Имя объекта политики, связанного с событием.
- **Информация** - Описание события, в том числе описание действий и ошибок.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, зарегистрировавшего событие.
- **ID-события** - Идентификационный номер события.

Примечание: Чтобы облегчить настройку фильтра, строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

- **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были зарегистрированы сервером.
- **Консолидация** - Поля для фильтрации по данным, относящимся к консолидации журналов (см. Консолидация журналов):
  - **Сервер** - Имя удаленного сервера, с которого данное событие было последний раз получено при консолидации журналов. Это поле нечувствительно к регистру и позволяет использовать знаки подстановки (* и ?). Используя точку с запятой в качестве разделителя, можно задать несколько значений.
  - **С**, **По** - Настройки временного диапазона для фильтрации событий по времени, когда они были последний раз получены с удаленного сервера при консолидации журналов.

Для каждого временного диапазона предусмотрены следующие настройки:

- **С** - Начало диапазона. Возможные значения:
  - **Первой записи** - Фильтровать события, начиная с самой ранней даты и времени в соответствующем поле журнала.
  - **Записи от** - Фильтровать события, начиная с определенной даты и времени.
- **По** - Конец диапазона. Возможные значения:
  - **Последнюю запись** - Фильтровать события, заканчивая самой поздней датой и временем в соответствующем поле журнала.
  - **Записи от** - Фильтровать события, заканчивая определенной датой и временем.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

13

Отчеты в DeviceLock

В этой главе:

Категории и типы отчетов

Задачи создания отчетов

Настройка электронной почты для доставки отчетов

Выбор формата отчетов по умолчанию

Работа с отчетами

Категории и типы отчетов

DeviceLock позволяет создавать отчеты на основе журналов сервера DeviceLock Enterprise Server. Отчеты предоставляют статистически обработанные данные о том, как сотрудники вашей компании используют те или иные устройства или сетевые протоколы. При создании отчета определяются его параметры, позволяющие выбирать данные для построения отчета. Например, можно указать отчетный период, за который будут отбираться данные для отчета.

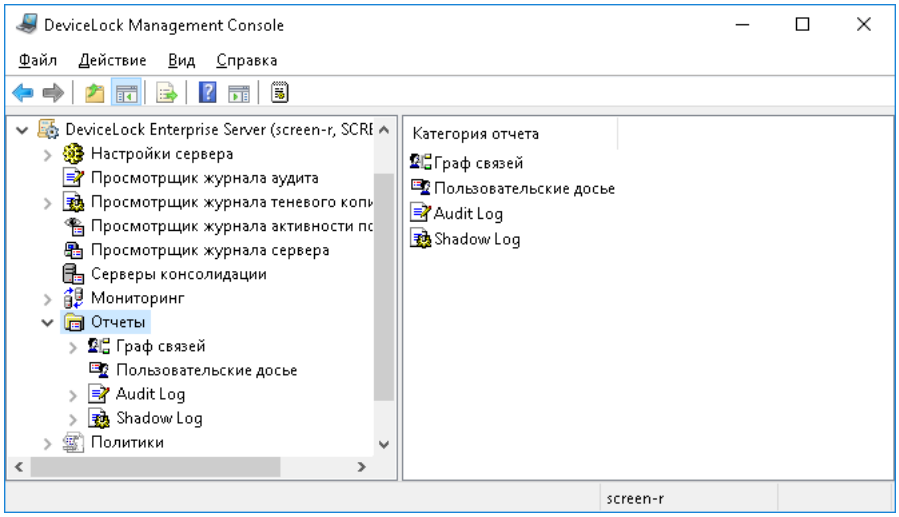
DeviceLock также позволяет создавать очень наглядные интерактивные отчеты (графы связей) для отображения и анализа коммуникаций сотрудников организации, основанные на данных о каналах коммуникации и частоте их использования. С помощью графа связей можно зрительно проанализировать кто, с кем, как часто и каким способом осуществлял коммуникации.

Отчеты можно создавать, посылать по электронной почте и сохранять в различных форматах. Отчеты создаются в консоли DeviceLock Management Console.

Предоставляются отчеты следующих категорий:

- Графы связей служат для интерактивного анализа коммуникационных взаимодействий сотрудников организации. Анализ проводится с помощью наглядных графических связей, которые строятся на основе данных о каналах коммуникации и частоте их использования.
- Пользовательские досье позволяют уполномоченным лицам отслеживать компьютерную активность пользователей с помощью удобного графического представления статистики их действий на компьютере. В этих отчетах предоставляются статистические показатели для мониторинга и оценки различных аспектов поведения пользователей, таких как частота попыток выполнить какие-либо несанкционированные действия или передать большие объемы данных, изменение сетевой активности пользователя и т.п.
- Отчеты по данным журнала аудита основаны на данных журналов событийного протоколирования, которые собирает и хранит DeviceLock Enterprise Server. Можно создавать только отчеты предопределенных типов, изменение или создание новых (пользовательских) типов не предусмотрено.
- Отчеты по данным журнала теневого копирования служат для анализа журналов теневого копирования, хранимых на сервере DeviceLock Enterprise Server. Все такие отчеты основаны на данных из журнала теневого копирования и журнала удаленных данных теневого копирования. Можно создавать только отчеты предопределенных типов, изменение или создание новых (пользовательских) типов не предусмотрено.

Категории отчетов отображаются под узлом **DeviceLock Enterprise Server** > **Отчеты** в дереве консоли:



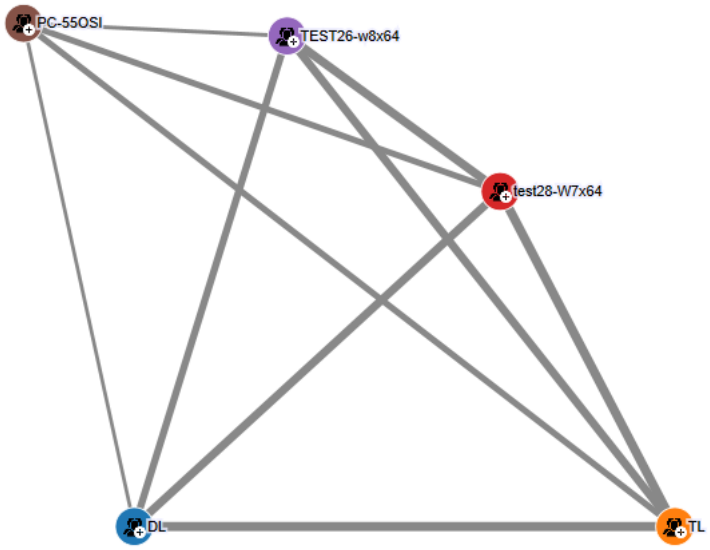
Контекстное меню узла **Отчеты** содержит следующие команды:

- **Настройки уведомления** - Настроить доставку отчетов по электронной почте (не относится к пользовательским досье и графам связей). Для этого требуется указать параметры SMTP-сервера и адреса получателей. Подробнее см. в разделе Настройка электронной почты для доставки отчетов.
- **Установить формат по умолчанию** - Выбрать выходной формат отчетов, который будет использоваться по умолчанию. Доступные варианты: HTML, PDF (выбран по умолчанию) и RTF. Выбор формата отчетов не влияет на пользовательские досье и графы связей. Подробнее см. в разделе Выбор формата отчетов по умолчанию.

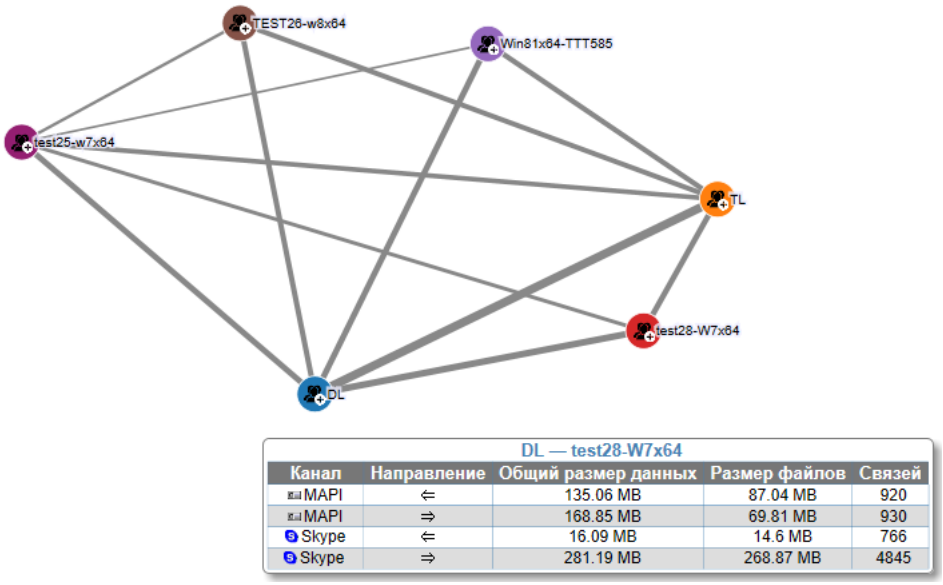
Графы связей

Графы связей позволяют исследовать статистику сетевой коммуникации пользователей путем анализа интерактивного графического представления данных, хранимых в журналах аудита (событийного протоколирования), теневого копирования и удаленных данных теневого копирования. Отчеты отображаются в форме графов. Для построения графов используются различные типы данных, включая данные о чатах, звонках и передаваемых файлах в сервисах мгновенных сообщений и социальных сетях, а также данные о сообщениях, передаваемых по электронной почте, включая вложения. Анализ данных производится для следующих сетевых протоколов: IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMTP, Социальные сети, Telegram, Viber, Web-почта, WhatsApp и Zoom. При построении графов могут не учитываться удаленные данные теневого копирования, относящиеся к размерам файлов, передаваемых через сервисы мгновенных сообщений, или в виде вложений, передаваемых по электронной почте.

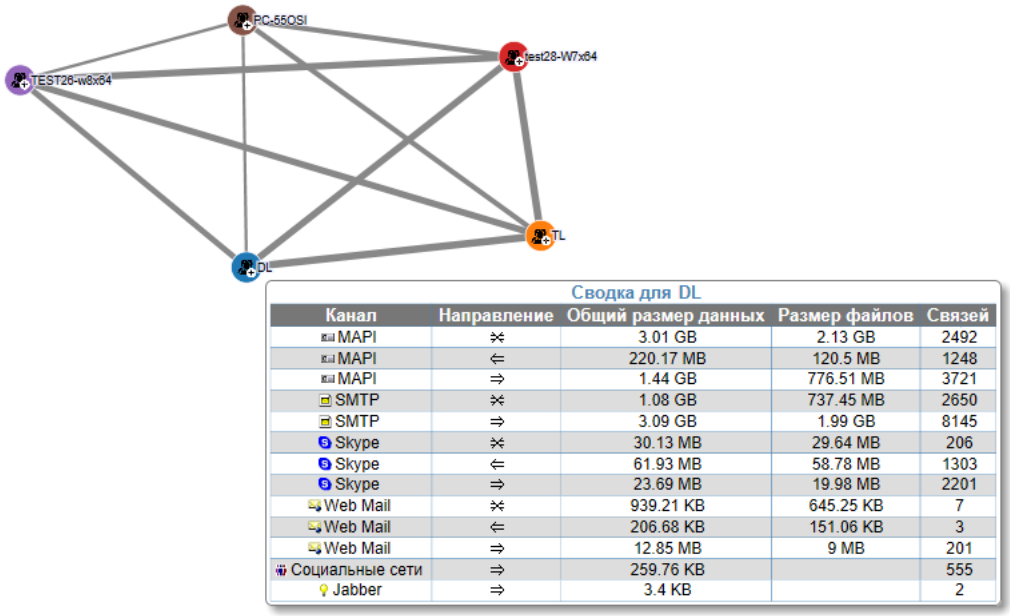
В состав графа входят два основных элемента: узлы (участники коммуникаций) и линии связей. Узлами представлены объекты Active Directory (AD), такие как домен, подразделение (OU) или пользователь. Линиями обозначаются связи или соединения между узлами. Толщина линии связи между двумя узлами отражает общее число коммуникаций между ними, включая количество чатов и переданных файлов в сервисах мгновенных сообщений, звонков, чатов в социальных сетях, а также количество сообщений и вложений, переданных по электронной почте. Тонкая линия означает незначительное число коммуникаций, толстая линия означает их большое количество.



При наведении указателя мыши на линию появляется всплывающее окно с информацией о связи между узлами, которые соединяет данная линия. Информация включает следующие сведения: канал коммуникации (напр., Skype, MAPI), направление коммуникации (входящая/исходящая), общий объем переданных данных, размер переданных файлов, а также число коммуникаций (таких как чаты и передача файлов в сервисах мгновенных сообщений, звонки Skype, чаты в социальных сетях, сообщения электронной почты, включая вложения) на канал.

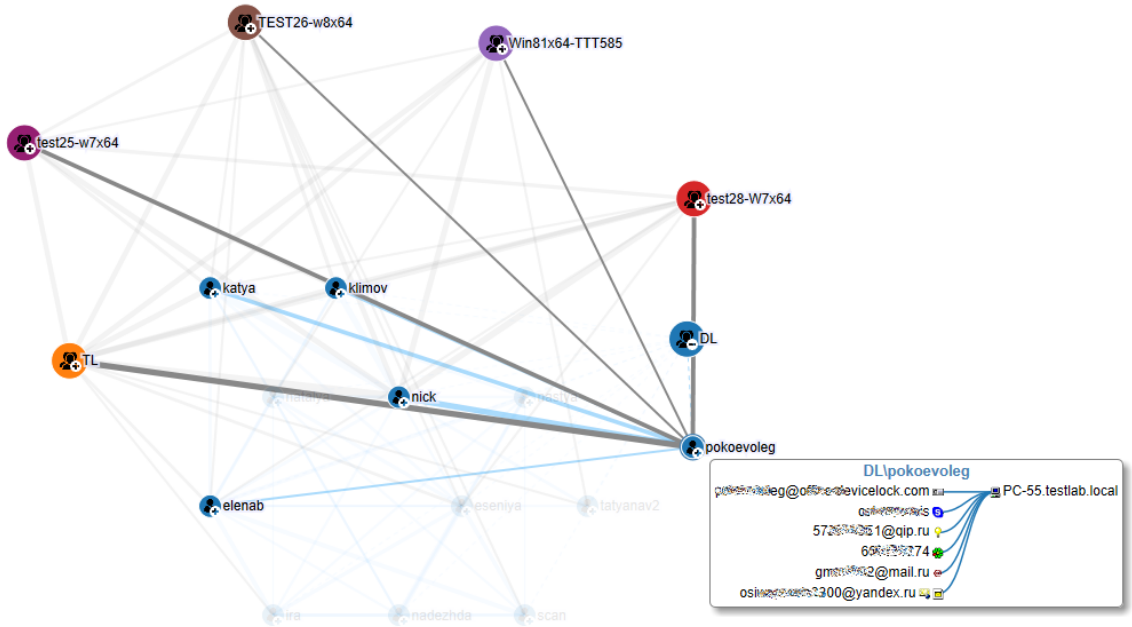


Графы представляют собой иерархические структуры. Узлы верхнего уровня обозначают домены организации. Все узлы верхнего уровня подкрашены различными цветами. Щелчок на значке «плюс» (+) в правом нижнем углу узла верхнего уровня раскрывает узлы уровнем ниже, которые представляют пользователей данного домена. Все узлы нижнего уровня подкрашены в тот же цвет, что и родительский узел верхнего уровня для упрощения наглядной идентификации пользователей определенного домена. Щелчок на значке «плюс» (+) в правом нижнем углу узла уровня пользователя раскрывает информацию об идентификаторах выбранного пользователя (такую как адреса электронной почты, идентификаторы социальных сетей и сервисов мгновенных сообщений) и данные о соединениях с другими пользователями. Чтобы свернуть раскрытый узел, следует щелкнуть на значке “минус” (-).



Канал	Направление	Общий размер данных	Размер файлов	Связей
MAPI	⇄	3.01 GB	2.13 GB	2492
MAPI	⇐	220.17 MB	120.5 MB	1248
MAPI	⇒	1.44 GB	776.51 MB	3721
SMTP	⇄	1.08 GB	737.45 MB	2650
SMTP	⇒	3.09 GB	1.99 GB	8145
Skype	⇄	30.13 MB	29.64 MB	206
Skype	⇐	61.93 MB	58.78 MB	1303
Skype	⇒	23.69 MB	19.98 MB	2201
Web Mail	⇄	939.21 KB	645.25 KB	7
Web Mail	⇐	206.68 KB	151.06 KB	3
Web Mail	⇒	12.85 MB	9 MB	201
Социальные сети	⇒	259.76 KB		555
Jabber	⇒	3.4 KB		2

При наведении указателя мыши на узел пользователя выводится всплывающее окно с информацией о данном пользователе. Эта информация включает имя пользователя в формате *DOMAIN\UserName* (например, *DL\katya*), имена компьютеров, которые он использует, а также идентификаторы пользователя (такие как адреса электронной почты, идентификаторы социальных сетей и сервисов мгновенных сообщений).



Пользователи в графах связей разделяются на два типа: внутренние и внешние. Внутренние пользователи - это пользователи внутри корпоративной сети, являющиеся членами домена организации; внешние пользователи - это пользователи вне корпоративной сети, не являющиеся членами домена организации. Внешние пользователи идентифицируются по адресам электронной почты или по идентификаторам социальных сетей и сервисов мгновенных сообщений.

Статистические данные по доменам и пользователям

Наведя указатель мыши на элемент отчета, можно получить дополнительную информацию об этом элементе. Для линий и пользовательских узлов такая информация отображается во всплывающем окне, как описано ранее в этом разделе. Всплывающее окно также появляется, если:

- Навести указатель мыши на узел домена (см. Статистика по доменам).
- Развернуть узел пользователя, и затем навести указатель мыши на любой из идентификаторов этого пользователя (см. Статистика по идентификаторам пользователей).
- Навести указатель мыши на узел **Уникальные** (см. Статистика по уникальным контактам).

Статистика по доменам

Если навести указатель мыши на узел, представляющий домен, отчет выводит сводную информацию о загрузке каналов сетевой коммуникации, вызванной всеми пользователями этого домена. Во всплывающем окне отображается имя домена, перечисляются каналы сетевой коммуникации и предоставляется следующая информация по каждому каналу:

- **Канал** - Протокол связи, такой как Skype, MAPI, SMTP, Web-почта, ICQ Messenger и т.п.
- **Направление** - Направление обмена данными:
  - Стрелка вправо (⇒) обозначает передачу данных пользователями домена внешним пользователям.
  - Стрелка влево (⇐) обозначает получение данных пользователями домена от внешних пользователей.
  - Двунаправленная стрелка (⇔) обозначает обмен данными между пользователями домена.
- **Общий размер данных** - Суммарный объем данных, переданных или полученных всеми пользователями домена через указанный канал в указанном направлении.
- **Размер файлов** - Суммарный размер файлов, переданных или полученных всеми пользователями домена через указанный канал в указанном направлении.
- **Связей** - Общее количество сеансов связи, использующих указанный канал в указанном направлении, которые были проведены всеми пользователями домена.

Статистика по идентификаторам пользователей

Если раскрыть узел, представляющий пользователя, а затем навести указатель мыши на идентификатор пользователя (например, адрес электронной почты или идентификатор сервиса мгновенных сообщений) в списке этого узла, отчет выводит сводную информацию о загрузке каналов сетевой коммуникации, вызванной этим идентификатором пользователя.

Появится всплывающее окно, в заголовке которого указан выбранный идентификатор пользователя и список идентификаторов пользователей, с которыми он осуществлял сетевую коммуникацию:

- Для внутреннего пользователя этот список содержит не более трех идентификаторов. Многоточие указывает, что список включает не все идентификаторы.
- Для идентификатора внешнего пользователя этот список содержит не более пяти имен доменных пользователей. Многоточие указывает, что список включает не все имена пользователей.

Во всплывающем окне перечислены каналы сетевой коммуникации данного идентификатора, и отображается следующая информация о каждом канале:

- **Канал** - Протокол связи, такой как Skype, MAPI, SMTP, Web-почта, ICQ Messenger и т.п.
- **Направление** - Направление обмена данными:
  - Стрелка вправо (⇒) обозначает передачу данных другим пользователям, как внутренним, так и внешним.
  - Стрелка влево (⇐) обозначает получение данных от других пользователей, как внутренних, так и внешних.
- **Общий размер данных** - Суммарный объем данных, переданных или полученных с помощью данного идентификатора пользователя через указанный канал в указанном направлении.
- **Размер файлов** - Суммарный размер файлов, переданных или полученных с помощью данного идентификатора пользователя через указанный канал в указанном направлении.
- **Связей** - Общее количество сеансов связи, проведенных с помощью данного идентификатора пользователя через указанный канал в указанном направлении.

Во всплывающем окне представлены сведения обо всех коммуникациях данного идентификатора, даже если этот идентификатор применяется к нескольким протоколам коммуникации. Однако объем данных, размер файлов и количество сеансов связи рассчитываются для каждого идентификатора отдельно. Значения, указанные для каждого протокола, относятся только к данному идентификатору, даже если у пользователя есть несколько идентификаторов для этого протокола.

Статистика по уникальным контактам

Если навести указатель мыши на узел **Уникальные** внутреннего пользователя, отчет выводит сводную информацию о загрузке каналов сетевой коммуникации, вызванной всеми уникальными контактами этого пользователя. Во всплывающем окне отображается доменное имя пользователя, перечисляются каналы сетевой коммуникации и предоставляется следующая информация по каждому каналу:

- **Канал** - Протокол связи, такой как Skype, MAPI, SMTP, Web-почта, ICQ Messenger и т.п.
- **Направление** - Направление обмена данными:
  - Стрелка вправо (⇒) обозначает передачу данных уникальным контактам пользователя.
  - Стрелка влево (⇐) обозначает получение данных от уникальных контактов пользователя.
- **Общий размер данных** - Суммарный объем данных, переданных или полученных уникальными контактами пользователя через указанный канал в указанном направлении.
- **Размер файлов** - Суммарный размер файлов, переданных или полученных уникальными контактами пользователя через указанный канал в указанном направлении.
- **Связей** - Общее количество сеансов связи, использующих указанный канал в указанном направлении, которые были проведены со всеми уникальными контактами пользователя.

Интерактивное управление графом

Интерактивное управление графом предполагает:

- **Увеличение и уменьшение масштаба.** Функция изменения масштаба позволяет изменять вид графа. Для изменения масштаба графа следует выполнить одно из следующих действий:
  - Прокрутить колесо мыши вперед или назад.
  - Удерживая нажатой клавишу `Ctrl`, нажать клавишу «плюс» (`+`) или «минус» (`-`).
- **Выбор одного или нескольких узлов графа.** Вид графа можно изменить путем выбора определенных узлов с целью их дальнейшего анализа. На графе выделяются только выбранные узлы, а также узлы, непосредственно соединенные с ними. Не выбранные узлы затеняются серым цветом. Можно выбрать один узел или несколько узлов щелчком мыши, удерживая при этом нажатой клавишу `Ctrl`.
- **Перемещение одного или нескольких узлов графа.** Узел графа можно переместить в менее загруженную область экрана, сохраняя при этом все его связи с другими узлами. Чтобы переместить узел, щелкните его и затем перетащите в нужное место, удерживая нажатой левую кнопку мыши.
- **Группирование уникальных контактов.** Уникальный контакт - это внешний пользователь, который ведет сетевые коммуникации только с одним внутренним пользователем. Возможно сгруппировать уникальные контакты пользователей (при их наличии в графе), для удобства и упрощения их поиска. Чтобы сгруппировать уникальные контакты, щелкните граф правой кнопкой мыши, и затем выберите **Группировать уникальные контакты**. Данные контактов (адреса электронной почты, идентификаторы социальных сетей и сервисов мгновенных сообщений) будут помещены в узел **Уникальные** для каждого внутреннего пользователя.

  Если уникальные контакты уже сгруппированы, применение команды **Группировать уникальные контакты** приводит к отмене их группирования. Поскольку уникальные контакты изначально сгруппированы, первое использование этой команды отменяет группирование уникальных контактов. Примените эту команду еще раз, чтобы восстановить группирование уникальных контактов.
- **Задание лимита отображения пользователей внутри узла.** Возможно задать количество пользователей, отображаемых в графе при раскрытии узла по щелчку на значке "плюс" (+). Для настройки числа пользователей, отображаемых при раскрытии узла, щелкните граф правой кнопкой мыши, затем выберите **Порог раскрытия пользователей/контактов**. В открывшемся диалоговом окне установите флаг **Порог раскрытия пользователей/контактов** и в поле **Порог** введите или выберите требуемое число пользователей (значение по умолчанию равно **20**). Если лимит количества отображаемых пользователей задан, вывод пользователей на граф начинается с контактов, с которыми выбранный пользователь имел наиболее частые коммуникации. Чтобы отобразить полный список контактов пользователя, щелкните значок "плюс" (+) в левом верхнем углу узла данного пользователя. Чтобы свернуть полный список контактов пользователя, щелкните значок "минус" (-) в правом нижнем углу узла данного пользователя.

  Лимит количества отображаемых пользователей применяется также к узлам, представляющим домены, и узлам **Уникальные**. Для просмотра полного списка, щелкните значок "плюс" (+) в левом верхнем углу данного узла. Чтобы свернуть полный список, щелкните значок "минус" (-) в правом нижнем углу данного узла.

Узел “Граф связей”

Графы связей создаются задачами, перечисленными в узле консоли **DeviceLock Enterprise Server** > **Отчеты** > **Граф связей**. Если выбрать такую задачу в дереве консоли, на панели сведений отображается список графов связей, созданных этой задачей. Подробнее см. в разделе Задачи создания отчетов.

В контекстном меню узла **Граф связей** предоставляются следующие команды:

- **Создать задачу** - Настроить новую задачу создания графа связей. Параметры задачи вводятся в появившихся диалоговых окнах.
- **Обновить** - Обновить список задач с учетом последних изменений.

Отчет “Граф связей”

Разверните узел, представляющий задачу создания графов связей (см. Задачи создания отчетов), для просмотра графов связей, созданных этой задачей. Выбранный в дереве консоли граф связей отображается на панели сведений. Описание данной категории отчетов см. в разделе Графы связей.

Если в дереве консоли выбрана задача создания графов связей, на панели сведений отображается список ее отчетов (графов связей). Подробнее об этом списке см. в разделе Просмотр отчетов, созданных задачей.

Контекстное меню графа связей предоставляет следующие команды:

- **Открыть** - Отобразить граф связей на панели сведений. Отобразить граф связей можно также, выбрав его в дереве консоли.
- **Переименовать** - Изменить имя графа связей.
- **Посмотреть параметры** - Открыть диалоговое окно для просмотра параметров отчета, которые были заданы для данного графа связей.
- **Удалить** - Удалить выбранный граф связей.
- **Обновить** - Обновить граф связей на панели сведений.

Пользовательские досье

Пользовательские досье - это мощное и простое в использовании решение, позволяющее отслеживать компьютерную активность пользователей с помощью удобного графического представления статистики их действий на компьютере.

Представленный в пользовательских досье статистический обзор онлайн-активности пользователей основан на различных показателях, которые дополняются данными LDAP-совместимых служб каталогов (в том числе службы доменов Active Directory). Пользовательские досье показывают частоту попыток совершения несанкционированных действий, передачи больших объемов данных, выявляют изменения в сетевой активности пользователей и т. д. Предоставляемые пользовательскими досье статистические данные помогают анализировать историю активности пользователей и выявлять типичные нарушения политик безопасности. Графическая визуализация статистических данных также дает удобный способ выявления наиболее активных пользователей.

Пользовательские досье предоставляют статистические индикаторы для мониторинга и оценки различных аспектов поведения пользователей, таких как частота попыток выполнить какие-либо несанкционированные действия или передать большие объемы данных, изменение активности пользователя и т.п. Благодаря этим показателям активность пользователей становится более прозрачной для мониторинга их действий с точки зрения информационной безопасности.

Пользовательские досье составляют единый каталог, охватывающий всю зарегистрированную сервисом DeviceLock статистику активности пользователей. Эти сведения накапливаются в базе данных сервера DeviceLock Enterprise Server для представления в пользовательских досье. Статистика пополняется по мере появления новых данных в журналах DeviceLock на сервере. Обновление статистики в пользовательских досье происходит автоматически во время низкой загруженности сервера, а также по расписанию.

Для отображения дополнительной информации о пользователях можно настроить соединение со службой доменов Active Directory или другой LDAP-совместимой службой каталогов. Сервер DeviceLock Enterprise Server получает данные пользователей из службы каталогов и добавляет их в пользовательские досье. При удалении пользователя из службы каталогов его досье не удаляется.

Пользовательские досье строятся по журналам аудита и теневого копирования, хранящимся на сервере DeviceLock Enterprise Server. Однако удаление записей из журналов не приводит к потере данных, уже зарегистрированных в пользовательском досье. После регистрации в досье статистические данные о действиях пользователей больше не зависят от журналов, из которых они были получены, т.к. пользовательские досье хранятся отдельно от журналов.

Данные пользовательских досье основаны на записях журнала теневого копирования и журнала аудита. В первую очередь используются записи журнала теневого копирования, а затем они дополняются данными из журнала аудита. Для полноты данных в пользовательских досье должно быть настроено теневое копирование.

Сворачивание событий

При построении пользовательских досье записи некоторых событий, произошедших в течение определенного порогового периода, объединяются в одно событие. Эта функция, известная как сворачивание событий, оптимизирует обработку данных о событиях и повышает точность пользовательских досье. Пороговый период составляет 10 секунд.

Учитывая, что одно действие пользователя часто вызывает несколько событий, сворачивание событий применяется при обработке данных из журнала аудита. Однотипные события, такие как разрешение доступа или запрет доступа, объединяются в одно событие, если выполнены все перечисленные условия:

- Разница времени событий не больше 10 секунд.
- Записи о событиях имеют одинаковые значения следующих полей: Сервер, Компьютер, Пользователь, Источник, Событие, PID, Процесс, Имя, Информация.

Сворачивание событий выполняется при построении любых диаграмм и списков на карточках пользователей.

Начало работы с пользовательскими досье

Администратор может просматривать пользовательские досье на панели сведений консоли DeviceLock Management Console, выбрав в дереве консоли **DeviceLock Enterprise Server** > **Отчеты** > **Пользовательские досье**. При отображении пользовательских досье панель сведений разделяется на две области:

- Список пользователей - Слева находится список пользователей и групп, полученных от сервера DeviceLock Enterprise Server.
- Карточка пользователя - Справа отображается карточка пользователя, выбранного из списка. На карточке приводятся данные учетной записи, а также статистика действий пользователя, зарегистрированных в журналах сервера DeviceLock Enterprise Server.

Пользовательские досье основаны на информации из журналов сервера DeviceLock Enterprise Server. Дополнительная информация для отображения на карточках пользователей может быть получена от службы каталогов (см. Настройки подключения к службе каталогов).

Список пользователей

В списке пользователей приводятся имена пользователей и групп. Группы представлены в виде контейнеров, содержащих пользователей - членов группы. Каждую группу можно раскрыть для просмотра списка содержащихся в ней пользователей.

Изначально список содержит только встроенные группы сервера DeviceLock Enterprise Server, например, группу **Все**, в которой содержатся все пользователи, зарегистрированные в журналах DeviceLock Enterprise Server. Можно создавать настраиваемые группы, добавляя туда пользователей вручную. Пользователя можно добавить в несколько групп.

Для работы со списком пользователей предусмотрены следующие элементы управления:

- Над списком находится поле быстрого поиска пользователей по имени (например, по имени и фамилии пользователя, или по имени его учетной записи). Введя какое-либо имя в это поле, можно быстро найти пользователей с таким именем.
- Группы в списке можно раскрывать. Дважды щелкните имя группы для просмотра пользователей, из которых она состоит. Затем щелкните имя пользователя, чтобы открыть его карточку.
- На каждой группе предусмотрено контекстное меню. Щелкните группу правой кнопкой мыши, а затем используйте следующие команды контекстного меню:
    - **Создать** - Создание настраиваемой группы.

      Настраиваемые группы могут быть полезны для анализа статистики пользователей с похожими профилями. Хорошей практикой является объединение таких пользователей в группы.
    - **Переименовать** - Переименование группы.

      Данная команда недоступна на встроенных группах (например, на группе **Все**). Имена встроенных групп определяются сервером. Изменение их вручную не допускается.
    - **Вставить** - Добавление пользователя из буфера обмена в группу. Вначале нужно скопировать пользователя в буфер обмена с помощью команды **Копировать**.

      Данная команда недоступна на встроенных группах (например, на группе **Все**). Состав встроенной группы определяется сервером. Изменение его вручную не допускается.
    - **Удалить** - Удаление группы. Эта команда не удаляет пользователей, входивших в состав группы.

      Данная команда недоступна на встроенных группах (например, на группе **Все**). Удаление встроенных групп не допускается.

- На каждом пользователе предусмотрено контекстное меню. Щелкните имя пользователя правой кнопкой мыши, а затем используйте следующие команды контекстного меню:
    - **Копировать** - Копирование пользователя в буфер обмена. Используйте эту команду совместно с командой **Вставить** из меню группы для добавления пользователей в настраиваемые группы.
    - **Удалить** - Удаление пользователя из настраиваемой группы. Эта команда не удаляет самого пользователя.

      Данная команда недоступна для пользователей во встроенных группах (например, в группе **Все**). Список участников встроенной группы определяется сервером. Изменение списка вручную не допускается.

Карточка пользователя

В списке пользователей каждую группу можно раскрыть для просмотра пользователей - членов данной группы. Рядом со списком отображается карточка пользователя, выбранного в этом списке.

Верхняя область карточки состоит из следующих элементов:

- Данные учетных записей пользователя
- Индикатор лояльности (нормальности) пользователя
- Обзор действий пользователя

После обзора действий пользователя на карточке представлена статистика использования устройств и протоколов данным пользователем. Эта часть карточки состоит из следующих элементов:

- Выбор отчетного периода
- Диаграммы активности пользователя
- Сведения о действиях пользователя
- Граф связей

На карточке пользователя имеется контекстное меню, позволяющее копировать текст в буфер обмена. Чтобы скопировать текст, выделите его на карточке пользователя и нажмите `Ctrl+C` или щелкните правой кнопкой мыши выделенный текст и выберите команду **Копировать**.

Данные учетных записей пользователя

В верхней части карточки приводится изображение (фото) пользователя, если его удалось получить из службы каталогов; в противном случае отображается общий значок пользователя.

Рядом с фото отображаются полученные от службы каталогов сведения о пользователе, в том числе список групп каталога, членом которых является данный пользователь (поле **Участник групп**). Затем перечисляются настраиваемые группы сервера DeviceLock Enterprise Server, в которые входит данный пользователь (поле **Группы**), а также все учетные записи данного пользователя, зарегистрированные в журналах на этом сервере (поле **Учетные записи**).

Так, на карточке пользователя домена Active Directory отображаются следующие сведения из службы каталогов Active Directory:

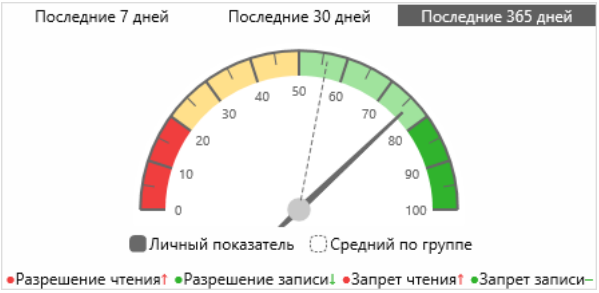
- Фото пользователя (photo)
- Отображаемое имя (displayName)
- Описание (description)
- Отдел (department)
- Адреса электронной почты (mail)
- Номер мобильного телефона (mobile)
- Имя руководителя (manager)
- Расположение офиса (physicalDeliveryOfficeName)
- Группы Active Directory, членом которых является данный пользователь (memberOf)

На карточке также перечисляются учетные записи, которые данный пользователь применял для доступа к ресурсам сети (протоколам), таким как веб-почта, службы обмена мгновенными сообщениями и т.п. Для каждой учетной записи отображается ее имя и значок протокола. Чтобы увидеть название протокола, наведите указатель мыши на значок протокола.

Примечание: Вместо учетных записей пользователя для социальных сетей на карточке перечисляются названия социальных сетей, к которым обращался данный пользователь.

Индикатор лояльности (нормальности) пользователя

На карточке отображается ряд показателей, обобщающих статистику действий пользователя за отчетный период с целью выявления аномалий или подозрительной активности. Эти показатели составляют индикатор лояльности (нормальности) пользователя. Индикатор лояльности помогает обнаруживать подозрительные действия пользователя и аномалии, указывая на отклонение поведения пользователя от определенного базового уровня.



Базовый уровень активности определяется как средний уровень активности пользователя за некоторый период, предшествующий отчетному. Продолжительность этого базового периода изменяется в зависимости от отчетного периода. Индикатор сравнивает средний уровень активности за отчетный период с базовым уровнем, позволяя выявить изменения в поведении пользователя и определить, действует ли он типично (показатель ближе к 100%) или аномально (показатель ближе к 0%). Возможные варианты отчетного периода: последние 7, 30 или 365 дней до текущей даты.

Продолжительность периода, на котором определяется базовый уровень, зависит от выбора отчетного периода:

Отчетный период	Продолжительность базового периода
Последние 7 дней	12 действительных 7-дневных интервалов до отчетного периода, либо все зарегистрированные в журналах дни до отчетного периода, если их меньше, чем 12 таких 7-дневных интервалов.
Последние 30 дней	12 действительных 30-дневных интервалов до отчетного периода, либо все зарегистрированные в журналах дни до отчетного периода, если их меньше, чем 12 таких 30-дневных интервалов.
Последние 365 дней	2 действительных 365-дневных интервала до отчетного периода, либо все зарегистрированные в журналах дни до отчетного периода, если их меньше, чем 2 таких 365-дневных интервала.

Действительными считаются только интервалы с ненулевой активностью пользователя. Для 7- и 30-дневного отчетного периода поиск таких интервалов ограничивается последним годом до отчетного периода. Если нет ни одного действительного интервала для базового периода или за отчетный период не зарегистрировано никакой активности пользователя, то на индикаторе отображается сообщение “Недостаточно данных”.

Для определения уровней активности определяются усредненные показатели количества действий, запрещенных и разрешенных сервисом DeviceLock, и затем вычисляется процент и направление изменений этих показателей по сравнению с базовым уровнем. Полученный результат отображается в качестве общего показателя нормальности, характеризующего изменение текущего уровня активности по сравнению с базовым. Более высокий показатель свидетельствует о лучшем соответствии действий пользователя политикам безопасности DeviceLock.

Пунктирной стрелкой на индикаторе пользователя отображается среднее значение по группе, позволяющее сравнить личный показатель лояльности пользователя со средним показателем лояльности его коллег. Подробнее см. в разделе Средний показатель по группе.

Индикатор пользователя содержит также показатели, уточняющие вклад различных типов пользовательской активности в изменение общего показателя:

- Разрешение чтения - Разрешенные попытки получения данных.
- Запрет чтения - Запрещенные попытки получения данных.
- Разрешение записи - Разрешенные попытки отправки данных.
- Запрет записи - Запрещенные попытки отправки данных.
- Поиск работы - Попытки использования сайтов поиска работы.

Уточняющий показатель отображается, только если изменился уровень соответствующей активности пользователя. Так, показатель поиска работы появляется в случае изменения уровня активности, связанной с использованием веб-сайтов поиска работы. Показатели разрешения чтения/записи или запрета чтения/записи появляются в случае изменения среднего количества разрешенных или запрещенных попыток обмена данными.

Для каждого из уточняющих показателей (кроме связанного с поиском работы) используются следующие обозначения того, как он изменился в отчетном периоде по сравнению с базовым уровнем:

- Стрелка вверх, красная - Рост количества разрешенных или запрещенных попыток.
- Стрелка вниз, зеленая - Снижение количества разрешенных или запрещенных попыток.
- Вертикальная черта, красная - Неизменное ненулевое количество разрешенных или запрещенных попыток.
- Вертикальная черта, зеленая - Неизменное количество разрешенных попыток и отсутствие запрещенных попыток.
- Длинный прочерк, зеленый - Отсутствие разрешенных / запрещенных попыток, что привело к росту общего показателя лояльности.

Средний показатель по группе

Личный показатель лояльности пользователя дополняется средним по группе, в которую входит данный пользователь. Средний показатель по группе представляет собой усредненное значение показателей лояльности пользователей - членов группы. При расчете среднего по группе крайние значения исходных данных отбрасываются для предотвращения искажений из-за самых высоких и самых низких показателей в группе.

Средний показатель по группе служит для сравнения показателя лояльности пользователя с показателями его коллег. Аномальное отклонение личного показателя от среднего по группе может указывать на подозрительную активность пользователя. Такая ситуация возникает, например, когда средний показатель находится в зеленой зоне, а показатель пользователя - за ее пределами.

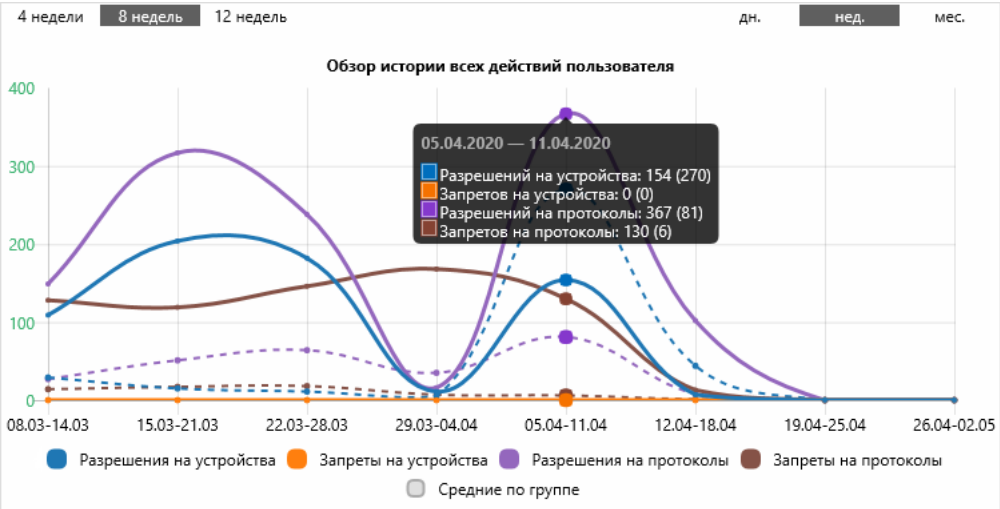
Средний показатель по группе отображается пунктирной стрелкой на той же диаграмме, что и показатель лояльности пользователя. Такой дизайн помогает сравнивать личный показатель пользователя со средним по группе.

Значение среднего показателя зависит от того, в какой группе выбран пользователь. Обратите внимание, что для выбора пользователя необходимо вначале раскрыть некоторую группу, а затем выбрать пользователя из этой группы. На индикаторе отображается средний показатель по той группе, которая использовалась для выбора пользователя.

Поскольку пользователь может быть членом нескольких групп, средний показатель может изменяться в зависимости от того, каким образом был выбран пользователь. Например, если пользователь выбран из списка членов встроенной группы **Все**, будет показано среднее значение по всем пользователям, зарегистрированным в журналах сервера. Если же выбрать пользователя из списка членов какой-либо настраиваемой группы, то будет показано среднее значение по пользователям - членам этой группы.

Обзор действий пользователя

На карточке отображается график **Обзор истории всех действий пользователя**, дающий представление об активности пользователя за определенный период.



Можно выбрать один из следующих периодов:

- Дни - Последние 7, 14 или 30 дней, включая текущий день. Каждый день представлен на горизонтальной оси маркером даты, над которым на графике отображаются суммарные показания за этот день.
- Недели - Последние 4, 8 или 12 недель, включая текущую неделю. Каждая неделя представлена на горизонтальной оси маркером даты начала/конца недели, над которым на графике отображаются суммарные показания за эту неделю.
- Месяцы - 12 месячных промежутков, предшествующих текущей дате. Каждый промежуток представлен на горизонтальной оси маркером даты его окончания, над которым на графике отображаются суммарные показания за этот промежуток.

Данный график дает представление о действиях пользователя за выбранный период с детализацией до одного дня. На нем отображаются несколько кривых, представляющих количество разрешенных и запрещенных действий пользователя:

- Разрешения на устройства - Количество разрешенных попыток доступа к устройствам.
- Запреты на устройства - Количество запрещенных попыток доступа к устройствам.
- Разрешения на протоколы - Количество разрешенных попыток доступа к протоколам.
- Запреты на протоколы - Количество запрещенных попыток доступа к протоколам.

Для просмотра числовых значений наведите указатель мыши на кривую над каким-либо маркером. Появится всплывающее окно, в котором указан выбранный маркер (день, неделя или месяц), а также количество разрешенных и запрещенных действий пользователя за время, соответствующее этому маркеру. В скобках указывается среднее количество соответствующих действий для группы, в которой выбран пользователь (см. Средние значения по группе).

По умолчанию на графике отображаются все кривые. Чтобы скрыть какую-либо кривую, нажмите ее идентификатор под графиком. Например, если вас интересуют только кривые запретов, вы можете скрыть кривые разрешений, нажав их идентификаторы. Чтобы снова отобразить кривую, нажмите ее идентификатор еще раз.

Каждая кривая на графике дополняется пунктирной кривой, представляющей средние значения по группе. Когда какая-либо из основных кривых скрыта, дополняющая ее кривая средних значений также не отображается.

Средние значения по группе

Помимо количества действий выбранного пользователя, на графике отображаются средние значения по группе, в которую входит данный пользователь. Каждое такое значение представляет собой среднее число определенных действий пользователей - членов группы (среднее число разрешенных / запрещенных попыток доступа к устройствам / протоколам). При расчете среднего по группе крайние значения исходных данных отбрасываются для предотвращения искажений из-за самых высоких и самых низких показателей в группе.

Средние значения по группе служат для сравнения показателей активности пользователя с соответствующими показателями активности его коллег. Аномальные отклонения от средних значений могут указывать на подозрительные действия пользователя. Такая ситуация возникает, например, когда количество запрещенных действий пользователя существенно выше среднего по группе.

Средние значения по группе отображаются пунктирными линиями соответствующего цвета. Например, среднее число запрещенных попыток доступа к устройствам отображается пунктирной линией того же цвета, что и кривая, представляющая количество запрещенных попыток пользователя получить доступ к устройствам. Такой дизайн облегчает сравнение показателей пользователя с их средними значениями по группе.

Если вас не интересуют средние значения, нажмите расположенную под графиком метку **Средние по группе**, чтобы скрыть эти сведения. Чтобы снова отобразить средние значения, нажмите эту метку еще раз.

Средние значения зависят от того, в какой группе выбран пользователь. Обратите внимание, что для выбора пользователя необходимо вначале раскрыть некоторую группу, а затем выбрать пользователя из этой группы. На графике будут отображены средние значения по той группе, которая использовалась для выбора пользователя.

Поскольку пользователь может быть членом нескольких групп, средние значения по группе могут изменяться в зависимости от того, каким образом был выбран пользователь. Например, если пользователь выбран из списка членов встроенной группы **Все**, средние значения вычисляются по всем пользователям, зарегистрированным в журналах сервера. Если же выбрать пользователя из списка членов какой-либо настраиваемой группы, то средние значения вычисляются только по пользователям - членам этой группы.

Выбор отчетного периода

На карточке отображается статистика действий пользователя за выбранный отчетный период. Диапазон дат отчетного периода определяет даты событий для включения в статистику. Статистика действий пользователя основана на данных о событиях, произошедших в отчетном периоде.

Селектор отчетного периода находится в верхней части области отображения статистики. Можно выбрать какой-либо предопределенный диапазон дат или использовать настраиваемый диапазон. Предусмотрены следующие предопределенные диапазоны дат:

- Сегодня - Текущая дата.
- Вчера - Дата, предшествующая текущей.
- Прошлая неделя - Диапазон дат с первого по последний день предыдущей календарной недели.
- Прошлый месяц - Диапазон дат с первого по последний день предыдущего календарного месяца.
- Последние 7 дней - Диапазон дат охватывает 7 дней, предшествующих текущей дате.
- Последние 30 дней - Диапазон дат охватывает 30 дней, предшествующих текущей дате.

Настраиваемый диапазон дат позволяет выбрать:

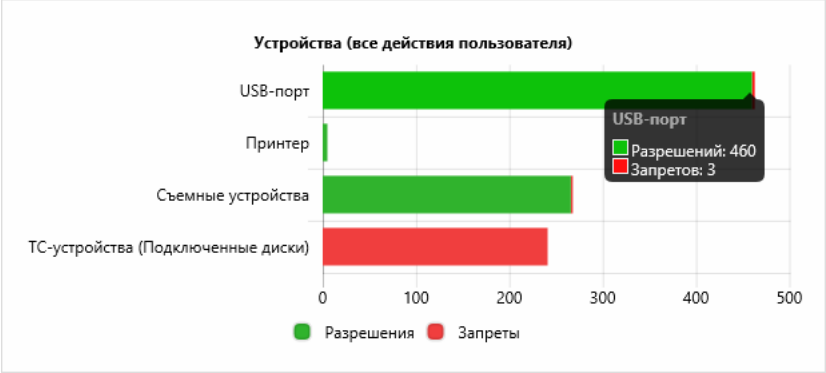
- Определенную дату - Для выбора щелкните требуемую дату мышкой.
- Непрерывный промежуток дат - Щелкните дату начала, а затем щелкните дату окончания требуемого промежутка дат.
- Все дни месяца - Для выбора щелкните название месяца в верхней части селектора.

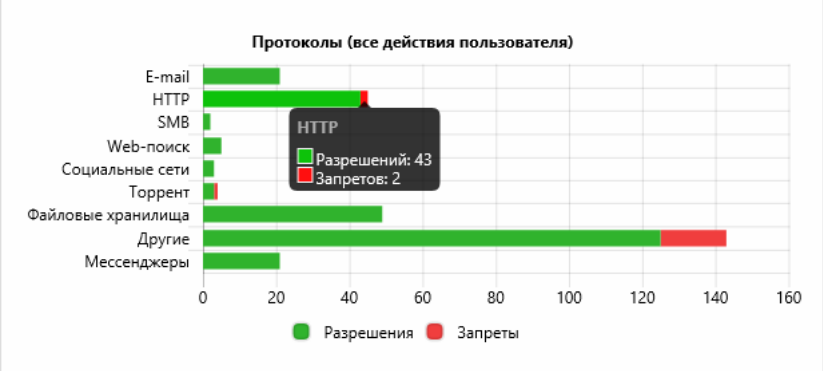
Закончив выбор желаемого диапазона дат, нажмите кнопку **OK**, чтобы изменение отчетного периода вступило в силу.

Для быстрого переключения отчетного периода используются команды рядом с селектором диапазона дат. Щелкните **Назад** или **Вперед**, чтобы переместить отчетный период назад или вперед во времени. Например, если выбран диапазон продолжительностью в одну неделю, эти команды перемещают отчетный период, соответственно, на неделю назад или на неделю вперед.

Диаграммы активности пользователя

Область статистики начинается с двух бар-диаграмм, представляющих разбивку количества разрешенных и запрещенных действий пользователя по типам устройств и по протоколам - под заголовками **Устройства (все действия пользователя)** и **Протоколы (все действия пользователя)**, соответственно. Для отображения количества действий на диаграммах используются горизонтальные полосы.





Каждая полоса диаграммы показывает количество разрешенных и запрещенных действий пользователя для некоторого канала передачи данных (типа устройств или протокола). Полоса "Tor-браузер" показывает количество попыток подключиться к сети Tor, запрещенных согласно настройке безопасности "Блокировать трафик Tor-браузера".

Некоторые полосы на диаграмме протоколов объединяют действия по нескольким каналам:

- **E-mail** - Протоколы SMTP, MAPI, IBM Notes или Web-почта.
- **Мессенджеры** - Протоколы обмена мгновенными сообщениями Skype, Jabber, Telegram, WhatsApp, Viber и т. п.
- **Proxy** - Прокси-серверы HTTP / SOCKS4 / SOCKS5. Объединяются действия, которые были запрещены согласно настройке безопасности "Блокировать прокси трафик".
- **Другие** - Неопознанные протоколы. Объединяются действия, зарегистрированные правилами белого списка для протокола Любой или SSL и/или правилами IP-файрвола. Здесь же учитываются действия, которые были запрещены согласно настройке безопасности "Блокировать нераспознанный исходящий SSL-трафик".

Наведите указатель мыши на такую "объединенную" полосу, чтобы просмотреть количество действий для каждого канала в отдельности.

Другие полосы относятся к отдельным типам устройств / протоколам. Отображаются только полосы, соответствующие устройствам и протоколам, для которых были зарегистрированы какие-либо действия пользователя.

Полоса диаграммы делится на два сегмента: зеленый представляет разрешенные действия, красный - запрещенные. Длина зеленого сегмента указывает количество разрешенных действий, длина всей полосы - суммарное количество действий, разрешенных и запрещенных. Для просмотра числовых значений наведите указатель мыши на какую-либо полосу. Появится всплывающее окно, в котором указан соответствующий этой полосе тип устройства или протокол, а также количество разрешенных и запрещенных действий пользователя для данного типа устройств или протокола за отчетный период.

Поскольку некоторые полосы объединяют действия по нескольким каналам передачи данных, на каждой такой полосе предусмотрено всплывающее окно для разбивки количества действий по каналам. В этом окне отображаются имена каналов, а также количество разрешенных и запрещенных действий пользователя для каждого канала.

Примечание: В отличие от пользовательских досье, учитывающих все зарегистрированные в журналах события, отчеты DeviceLock могут не учитывать некоторые события. Например, отчеты “Read & Write access requests per device type” и “Allowed & Denied access requests per channel” не учитывают события Подключение и Отключение для USB-устройств. По этой причине показания отчетов могут отличаться от показаний графика истории и диаграмм активности в карточке пользователя.

Сведения о действиях пользователя

За диаграммами активности пользователя следуют списки файлов (не более 10 файлов в списке), которые пользователь пытался отправить, получить, или распечатать на принтере. Содержимое списков зависит от того, в каких журналах DeviceLock зарегистрированы файлы. Для файлов, зарегистрированных в журнале теневого копирования, можно получить списки самых больших файлов, а также размеры таких файлов. Для файлов, зарегистрированных в журнале аудита, можно получить списки файлов, которые пользователь чаще всего пытался отправить, получить или распечатать, а также количество таких попыток. Предоставляются следующие списки файлов:

- Топ-10 типов входящих и исходящих файлов по размеру файла - Списки, состоящие из двух столбцов. В первом столбце перечисляются типы файлов. Для каждого типа приводится его описание. Во втором столбце указывается суммарный размер файлов каждого типа. Может отображаться четыре списка:
  - **Топ типов разрешенных входящих файлов** - Типы файлов, получение которых было разрешено.
  - **Топ типов запрещенных входящих файлов** - Типы файлов, получение которых было запрещено.
  - **Топ типов разрешенных исходящих файлов** - Типы файлов, отправка которых была разрешена.
  - **Топ типов запрещенных исходящих файлов** - Типы файлов, отправка которых была запрещена.

  Каждый список содержит не более 10 типов файлов наибольшего суммарного размера. Списки основаны на данных из журнала теневого копирования. Если в журнале нет данных, относящихся к определенной категории файлов (Разрешенные / Запрещенные, Входящие / Исходящие), то соответствующий список не отображается.
- Топ-10 входящих и исходящих файлов по размеру файла или по количеству попыток - Списки, состоящие из двух столбцов. В первом столбце перечисляются имена файлов, которые пользователь пытался отправить или получить. Во втором столбце указывается либо размер файла, либо количество попыток отправить или получить этот файл. Может отображаться четыре списка:
  - **Топ разрешенных входящих файлов** - Файлы, получение которых было разрешено.
  - **Топ запрещенных входящих файлов** - Файлы, получение которых было запрещено.
  - **Топ разрешенных исходящих файлов** - Файлы, отправка которых была разрешена.
  - **Топ запрещенных исходящих файлов** - Файлы, отправка которых была запрещена.

  Каждый список содержит не более 10 файлов наибольшего размера или не более 10 файлов с наибольшим количеством попыток отправки или получения. Списки, в которых приводятся размеры файлов, основаны на данных из журнала теневого копирования. Списки, показывающие количество попыток, основаны на данных из журнала аудита. Если в журнале нет данных, относящихся к определенной категории файлов (Разрешенные / Запрещенные, Входящие / Исходящие), то соответствующий список не отображается.

Для переключения между просмотром списка по размеру файла / количеству попыток, щелкните следующий элемент в заголовке списка:

- Щелкните **Показать по количеству**, чтобы просмотреть список файлов с наибольшим количеством попыток.
- Щелкните **Показать по размеру**, чтобы просмотреть список файлов наибольшего размера.

Такое переключение возможно, если журнал теневого копирования содержит достаточно данных для построения списка файлов. В противном случае файлы включаются в список по количеству попыток отправки / получения, а элементы **Показать по количеству** и **Показать по размеру** не отображаются.

- Топ-10 печатаемых файлов по размеру файла или по количеству попыток - Списки, состоящие из двух столбцов. В первом столбце перечисляются имена файлов, которые пользователь пытался распечатать на принтере. Во втором столбце указывается либо размер файла, либо количество попыток распечатать этот файл. Может отображаться два списка:

  - **Топ разрешенных к печати файлов** - Файлы, которые было разрешено распечатать на принтере.
  - **Топ запрещенных к печати файлов** - Файлы, которые было запрещено распечатать на принтере.

  Каждый список содержит не более 10 файлов наибольшего размера или не более 10 файлов с наибольшим количеством попыток распечатать файл на принтере. Списки, в которых приводятся размеры файлов, основаны на данных из журнала теневого копирования. Списки, показывающие количество попыток, основаны на данных из журнала аудита. Если в журнале нет данных, относящихся к определенной категории файлов (Разрешенные / Запрещенные), то соответствующий список не отображается.

  Для переключения между просмотром списка по размеру файла / количеству попыток, щелкните следующий элемент в заголовке списка:

  - Щелкните **Показать по количеству**, чтобы просмотреть список файлов с наибольшим количеством попыток.
  - Щелкните **Показать по размеру**, чтобы просмотреть список файлов наибольшего размера.

  Такое переключение возможно, если журнал теневого копирования содержит достаточно данных для построения списка файлов. В противном случае файлы включаются в список по количеству попыток печати, а элементы **Показать по количеству** и **Показать по размеру** не отображаются.

Далее на карточке приводятся два списка правил, которые запрещали или разрешали данному пользователю передавать определенный контент / обнаруживали передачу контента (контентно-зависимые правила):

- **Топ разрешающих контентно-зависимых правил** - Наиболее часто срабатывающие правила разрешения или обнаружения передачи контента.
- **Топ запрещающих контентно-зависимых правил** - Наиболее часто срабатывающие правила запрета передачи контента.

Количество срабатываний каждого правила подсчитывается совместно для устройств и протоколов. Правила обнаружения контента считаются правилами, которые разрешают передачу контента.

В список включаются до 10 правил. Для каждого правила отображается его имя и общее количество срабатываний.

Затем на карточке приводятся сведения об обмене файлами и данным с контактами пользователя:

- **Топ контактов** - Контакты, с которыми пользователь чаще всего обменивался файлами и данными. Для каждого контакта в списке предоставляются следующие сведения:
    - Имя контакта.
    - Суммарный объем данных, отправленных данному контакту или полученных от него. Отображается только при наличии соответствующих данных в журнале аудита и/или теневого копирования.
    - Суммарный размер файлов, отправленных данному контакту или полученных от него. Отображается только при наличии соответствующих данных в журнале аудита и/или теневого копирования.
    - Общее количество коммуникаций с данным контактом.

В список включаются до 10 контактов с наибольшим количеством коммуникаций.

Граф связей

Область статистики завершается диаграммой, которая позволяет просматривать взаимосвязи и обмен данными между пользователем и его контактами посредством графического представления данных из журналов DeviceLock за отчетный период. Для построения диаграммы используются данные о чатах и передаваемых файлах в службах мгновенных сообщений, данные о звонках Skype и чатах в социальных сетях, а также данные о сообщениях, передаваемых по электронной почте, включая почтовые вложения. При этом учитываются данные, передаваемые по различным протоколам, в том числе IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMTP, Социальные сети, Telegram, Viber, Web-почта, WhatsApp и Zoom.

Диаграмма представлена в виде графа, состоящего из двух основных компонентов:

- Узлы - Один из узлов представляет пользователя, а остальные узлы представляют контакты этого пользователя.
- Линии связей между узлами - Каждая линия представляет собой связь между пользователем и одним из его контактов. Ее толщина пропорциональна общему количеству коммуникаций пользователя с данным контактом.

При наведении указателя мыши на линию появляется всплывающее окно с информацией о связи между узлами, которые соединяет данная линия. Информация включает следующие сведения: канал коммуникации (например, Skype, MAPI), направление коммуникации (входящая/исходящая), общий объем переданных данных, размер переданных файлов, а также число коммуникаций (таких как чаты и передача файлов в сервисах мгновенных сообщений, звонки Skype, чаты в социальных сетях, сообщения электронной почты, включая вложения) на канал.

При наведении указателя мыши на узел появляется всплывающее окно с информацией о пользователе или контакте. В зависимости от типа узла эта информация может содержать имя пользователя или контакта, имя компьютера пользователя и идентификаторы пользователя или контакта (такие как адреса электронной почты, идентификаторы социальных сетей и сервисов мгновенных сообщений).

Подробнее о графах связей см. в разделе Графы связей.

Настройки подключения к службе каталогов

В меню узла **Пользовательские досье** предусмотрена команда для настройки подключения к LDAP-совместимой службе каталогов (например, Active Directory или OpenLDAP). Такое подключение расширяет пользовательские досье дополнительными сведениями о пользователях из службы каталогов (см. Данные учетных записей пользователя).

При отсутствии подключения к службе каталогов пользовательские досье основываются только на информации, содержащейся в записях журналов DeviceLock Enterprise Server.

Пользовательские досье автоматически подключаются к службе каталогов Active Directory, если компьютер сервера DeviceLock Enterprise Server находится в домене Active Directory. Для доступа к службе каталогов Active Directory в этом случае по умолчанию используется учетная запись входа в систему службы DeviceLock Enterprise Server, заданная параметром Входить в систему как. Если прав доступа у этой учетной записи недостаточно, можно указать другую учетную запись в диалоговом окне настройки подключения к службе каталогов.

Пользовательские досье получают обновленную информацию из службы каталогов ежесуточно в 1 час ночи по местному времени сервера DeviceLock Enterprise Server, а также при каждом запуске службы DeviceLock Enterprise Server.

Для настройки подключения к службе каталогов

1. В дереве консоли выберите **DeviceLock Enterprise Server** > **Отчеты** > **Пользовательские досье**.
2. Щелкните правой кнопкой мыши **Пользовательские досье** и выберите команду **Параметры службы каталогов**.
3. Используйте появившееся Диалоговое окно настройки подключения к службе каталогов, чтобы задать, просмотреть или изменить параметры подключения.

Диалоговое окно настройки подключения к службе каталогов

Команда **Параметры службы каталогов** открывает диалоговое окно для ввода, просмотра или изменения параметров подключения к LDAP-совместимой службе каталогов. Эти параметры зависят от выбранной службы каталогов:

- Active Directory - Данные учетной записи для доступа к домену Active Directory.
- LDAP - Данные учетной записи и другие параметры для подключения к серверу LDAP.

Active Directory

Параметры Active Directory применяются, когда компьютер сервера DeviceLock Enterprise Server находится в домене Active Directory, но учетная запись входа в систему службы DeviceLock Enterprise Server не обладает правами доступа к службе каталогов Active Directory. В таком случае можно указать учетную запись пользователя с достаточными правами для получения данных от службы каталогов Active Directory. Также возможно подключение к определенному домену Active Directory, что может потребоваться, когда DeviceLock Enterprise Server работает на компьютере, который не присоединен к домену (автономный сервер), или данные пользователей необходимо получить из другого домена.

Диалоговое окно содержит следующие поля для указания домена Active Directory и для ввода имени и пароля пользователя домена:

- **Хост** - Любое из следующих значений:
  - Полное доменное имя (FQDN) домена Active Directory.
    Пример: `production.company.com`
  - Имя или IP-адрес сервера, на котором работает контроллер домена Active Directory.
    Пример: `dc1.production.company.com`

    Контроллер домена можно выбрать из списка, нажав кнопку ... рядом с этим полем.

  Примечание: Если хост не указан, пользовательские досье либо подключаются к любому доступному контроллеру того домена, к которому присоединен компьютер сервера DeviceLock Enterprise Server, либо не подключаются к службе каталогов Active Directory (в случае автономного сервера).

- **Имя пользователя** - Допускается имя пользователя в любом из следующих форматов:
  - `user@domain` - Здесь `user` обозначает имя учетной записи пользователя, а `domain` - UPN-суффикс домена.
  - `domain\user` - Здесь `domain` обозначает короткое (NetBIOS) имя домена, а `user` - имя пользователя для входа в домен.
- **Пароль** - Пароль учетной записи пользователя в домене.

  Примечание: Если имя пользователя не указано, то для доступа к службе каталогов Active Directory используется учетная запись входа в систему службы DeviceLock Enterprise Server, заданная параметром Входить в систему как.

LDAP

Диалоговое окно содержит следующие поля для ввода параметров подключения к серверу LDAP (например, для подключения к серверу OpenLDAP или AD LDS):

- **Хост** - Имя или IP-адрес LDAP-сервера. Сервер можно выбрать из списка, нажав кнопку ... рядом с этим полем.
- **Порт** - Номер используемого LDAP-сервером TCP-порта, по умолчанию - 389.
- **Базовый DN** - Начальная точка для просмотра дерева каталогов. Это должно быть действительное DN-имя, например `cn=users,o=company,c=US`. Если базовый DN не указан, просмотр начинается с корня дерева. Нажмите кнопку **Получить**, чтобы выбрать контекст именования для базового DN.
- **Пользовательский DN**, **Пароль** - DN-имя и пароль пользователя службы каталогов для доступа к LDAP-серверу. Пользовательский DN должен быть действительным DN-именем, например `cn=admin,o=company,c=US`.

  Примечание: Если пользовательский DN не указан, то для доступа к LDAP-серверу используется учетная запись входа в систему службы DeviceLock Enterprise Server, заданная параметром Входить в систему как.

Отчеты по данным журнала аудита

Отчеты по данным журнала аудита основаны на записях журнала аудита (**Audit Log**) сервера DeviceLock Enterprise Server. В этой категории предусмотрены следующие типы отчетов:

- 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

В консоли под каждым типом отчетов перечисляются задачи создания отчетов данного типа. Например, задачи создания отчетов Top active computers категории Audit Log перечисляются в узле консоли **DeviceLock Enterprise Server** > **Отчеты** > **Audit Log** > **Top active computers**. Если выбрать задачу в дереве консоли, на панели сведений отображается список отчетов, созданных этой задачей. Подробнее см. в разделе Задачи создания отчетов.

Allowed & Denied access requests per channel

Этот отчет показывает количество разрешенных и запрещенных попыток доступа по каналам передачи данных (устройства и/или протоколы).

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **User(s)** - Пользователи, выбранные для отчета.
- **Channel(s)** - Каналы передачи данных, выбранные для отчета. Возможные варианты: **all devices** (все устройства), **all protocols** (все протоколы) и **all devices and protocols** (все устройства и протоколы).

Примечание:

- Отчеты для **all protocols** или **all devices and protocols** могут содержать запись о протоколе **Другие** (Other), в которой суммируются запросы на доступ через протоколы неопознанного типа, зарегистрированные правилами белого списка протоколов (протоколы **Любой** или **SSL**) и/или правилами IP-файрвола.
- Если действует настройка безопасности **Блокировать трафик Tor-браузера**, попытки использовать Tor-браузер учитываются как запрещенные запросы на доступ через протокол **Другие**.

Раздел “Результаты отчета” содержит таблицу и диаграмму, которые представляют обработанные данные в отчете. Таблица содержит следующие столбцы:

- **Channel** - Канал передачи данных.
- **Allowed** - Количество разрешенных попыток доступа к устройствам и/или протоколам.
- **Denied** - Количество запрещенных попыток доступа к устройствам и/или протоколам.

Allowed vs. Denied access requests

Этот отчет показывает общее количество разрешенных и запрещенных попыток доступа для всех каналов передачи данных.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **User(s)** - Пользователи, выбранные для отчета.
- **Channel(s)** - Каналы передачи данных, выбранные для отчета. Возможные варианты: **all devices** (все устройства), **all protocols** (все протоколы) и **all devices and protocols** (все устройства и протоколы).

Примечание:

- Отчеты для **all protocols** или **all devices and protocols** могут содержать запись о протоколе **Другие** (Other), в которой суммируются запросы на доступ через протоколы неопознанного типа, зарегистрированные правилами белого списка протоколов (протоколы **Любой** или **SSL**) и/или правилами IP-файрвола.
- Если действует настройка безопасности **Блокировать трафик Tor-браузера**, попытки использовать Tor-браузер учитываются как запрещенные запросы на доступ через протокол **Другие**.

Раздел “Результаты отчета” содержит таблицу и круговую диаграмму, которые представляют обработанные данные в отчете. Таблица содержит следующие строки:

- **Allowed** - Общее количество разрешенных попыток доступа к устройствам и протоколам и соответствующий процент.
- **Denied** - Общее количество запрещенных попыток доступа к устройствам и протоколам и соответствующий процент.
- **Total** - Общее количество всех попыток доступа к устройствам и протоколам и соответствующий процент.

Круговая диаграмма отображает данные в виде процентных долей.

Read & Write access requests per device type

Этот отчет показывает количество попыток чтения и записи по типам устройств. Отчет содержит данные только по следующим типам устройств: Гибкий диск, iPhone-устройства, MTP, Съемные устройства, TC-устройства, Буфер обмена, Жесткий диск, Оптический привод, Ленточные накопители, Windows Mobile и Palm.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Access Type(s)** - Типы событий, выбранных для отчета.
- **Computer(s)** - Компьютеры, выбранные для отчета.
- **User(s)** - Пользователи, выбранные для отчета.

Раздел “Результаты отчета” содержит таблицу и диаграмму, которые представляют обработанные данные в отчете. Таблица содержит следующие столбцы:

- **Device Type** - Тип устройства.
- **Read** - Количество попыток чтения.
- **Write** - Количество попыток записи.

Таблица также содержит строку **Total**, которая суммирует все значения в столбцах **Read** и **Write**.

Top active computers

Этот отчет показывает список наиболее часто используемых компьютеров, отсортированный по количеству разрешенных и запрещенных попыток доступа к устройствам и протоколам. По умолчанию, отчет отображает первые 10 компьютеров, но можно указать любое число компьютеров.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.

  Примечание:
  - В отчетах, для которых выбран протокол **Другие**, учитываются также запросы на доступ через протоколы неопознанного типа. Такие запросы регистрируются правилами белого списка протоколов (протоколы **Любой** или **SSL**) и правилами IP-файрвола.
  - Если действует настройка безопасности **Блокировать трафик Tor-браузера**, то в отчетах, для которых выбран протокол **Другие**, учитываются также попытки использовать Tor-браузер (расцениваются как запрещенные запросы на доступ через протокол **Другие**).

Раздел “Результаты отчета” содержит две таблицы, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) компьютеров с разрешенными попытками доступа. Таблица 2 содержит список первых N (где N - заданное число) компьютеров с запрещенными попытками доступа. Эти таблицы включают следующие столбцы:

- **Computer Name** - Имя компьютера.
- **Access Count** - Количество попыток доступа. Значения в этом столбце упорядочены по убыванию.

Top active processes

Этот отчет показывает список наиболее активных процессов (приложений), отсортированный по количеству разрешенных и запрещенных попыток доступа к устройствам и протоколам. По умолчанию, отчет отображает первые 10 процессов, но можно указать любое число процессов.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.

Примечание:

- В отчетах, для которых выбран протокол **Другие**, учитываются также запросы на доступ через протоколы неопознанного типа. Такие запросы регистрируются правилами белого списка протоколов (протоколы **Любой** или **SSL**) и правилами IP-файрвола.
- Если действует настройка безопасности **Блокировать трафик Tor-браузера**, то в отчетах, для которых выбран протокол **Другие**, учитываются также попытки использовать Tor-браузер (расцениваются как запрещенные запросы на доступ через протокол **Другие**).

Раздел “Результаты отчета” содержит две таблицы, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) процессов с разрешенными попытками доступа. Таблица 2 содержит список первых N (где N - заданное число) процессов с запрещенными попытками доступа. Эти таблицы включают следующие столбцы:

- **Process Name** - Имя процесса.
- **Access Count** - Количество запросов на доступ. Значения в этом столбце упорядочены по убыванию.

Top active users

Этот отчет показывает список наиболее активных пользователей, отсортированный по количеству разрешенных и запрещенных попыток доступа к устройствам и протоколам. По умолчанию, отчет отображает первые 10 пользователей, но можно указать любое число пользователей.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.

Примечание:

- В отчетах, для которых выбран протокол **Другие**, учитываются также запросы на доступ через протоколы неопознанного типа. Такие запросы регистрируются правилами белого списка протоколов (протоколы **Любой** или **SSL**) и правилами IP-файрвола.
- Если действует настройка безопасности **Блокировать трафик Tor-браузера**, то в отчетах, для которых выбран протокол **Другие**, учитываются также попытки использовать Tor-браузер (расцениваются как запрещенные запросы на доступ через протокол **Другие**).

Раздел “Результаты отчета” содержит две таблицы, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) пользователей с разрешенными попытками доступа. Таблица 2 содержит список первых N (где N - заданное число) пользователей с запрещенными попытками доступа. Эти таблицы содержат следующие столбцы:

- **User Name** - Имя пользователя.
- **Access Count** - Количество попыток доступа. Значения в этом столбце упорядочены по убыванию.

Top inserted USB & FireWire devices

Этот отчет показывает 3 группы часто используемых USB- и FireWire-устройств, отсортированный по количеству событий Insert (“Подключение”).

- Группа 1 содержит как разрешенные, так и запрещенные устройства.
- Группа 2 содержит только разрешенные устройства.
- Группа 3 содержит только запрещенные устройства.

По умолчанию, отчет отображает первые 10 устройств в каждой группе, но можно указать любое число устройств.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.

Раздел “Результаты отчета” содержит три таблицы, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) подключенных USB- и Firewire-устройств (как разрешенных, так и запрещенных). Таблица 2 содержит список первых N (где N - заданное число) разрешенных USB- и FireWire-устройств. Таблица 3 содержит список первых N (где N - заданное число) запрещенных USB- и FireWire-устройств. Эти таблицы содержат следующие столбцы:

- **Device Name** - Имя устройства.
- **Insert Count** - Количество событий “Подключение”. Значения в этом столбце упорядочены по убыванию.

Top used USB devices

Этот отчет содержит три группы наиболее используемых USB-устройств исходя из количества попыток доступа:

- Группа 1 содержит как разрешенные, так и запрещенные устройства.
- Группа 2 содержит только разрешенные устройства.
- Группа 3 содержит только запрещенные устройства.

По умолчанию, отчет отображает первые 10 устройств в каждой группе, но можно указать любое число устройств.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.

Раздел “Результаты отчета” содержит три таблицы, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) USB-устройств с разрешенным и запрещенным доступом. Таблица 2 содержит список первых N (где N - заданное число) USB-устройств, к которым совершались успешные попытки доступа. Таблица 3 содержит список первых N (где N - заданное число) USB-устройств, к которым попытки доступа отклонялись. Эти таблицы включают следующие столбцы:

- **Device Name** - Имя устройства.
- **Access Count** - Количество попыток доступа. Значения в этом столбце упорядочены по убыванию.

DeviceLock Service versions

Этот отчет показывает общее количество компьютеров с указанной версией сервиса DeviceLock и количество компьютеров, которые имеют разные номера сборок для каждой версии.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Version(s)** - Версии сервиса DeviceLock, выбранные для отчета.

Раздел “Результаты отчета” содержит таблицу и круговую диаграмму, которые представляют обработанные данные в отчете. Таблица содержит следующие столбцы:

- **Version** - Отображает номер версии.
- **Build** - Отображает номер сборки. Значения в этом столбце упорядочены по убыванию.
- **Number of Computers** - Отображает количество компьютеров, имеющих определенный номер сборки, и общее количество компьютеров с определенными версиями сервиса DeviceLock.

На круговой диаграмме отображаются процентные доли компьютеров с указанными версиями сервиса DeviceLock.

DeviceLock Service versions by computers

Этот отчет содержит список указанных версий сервиса DeviceLock и имена компьютеров, а также общее количество компьютеров для каждой версии.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Version(s)** - Версии сервиса DeviceLock, выбранные для отчета.

Раздел “Результаты отчета” содержит таблицу, которая представляет обработанные данные в отчете. Таблица содержит следующие столбцы:

- **Version** - Отображает номер версии.
- **Computer name** - Отображает имена компьютеров и общее количество компьютеров для каждой указанной версии.

DeviceLock policy changes

Этот отчет показывает список событий, связанных с изменениями политик.

Отчет состоит из трех разделов “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

Раздел “Заголовок отчета” содержит имя отчета, отображаемое в начале отчета. Имя отчета совпадает с типом отчета.

Раздел “Параметры отчета” содержит информацию о параметрах отчета, заданных при формировании отчета. Эта информация включает:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.

Раздел “Результаты отчета” содержит таблицу, которая представляет обработанные данные в отчете. Таблица содержит следующие столбцы:

- **Date/time** - Время и дата изменения политики.
- **Action** - Детальная информация о событии изменения политики.
- **User** - Пользователь, внесший изменения в политику.

Top used Printers

Этот отчет содержит три группы наиболее часто используемых принтеров исходя из количества запросов на доступ:

- Группа 1 содержит как разрешенный, так и запрещенный доступ.
- Группа 2 содержит только разрешенный доступ.
- Группа 3 содержит только запрещенный доступ.

По умолчанию, отчет отображает первые 10 принтеров в каждой группе, но можно указать любое число принтеров.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.

Раздел “Результаты отчета” содержит три таблицы, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) принтеров с разрешенным и запрещенным доступом. Таблица 2 содержит список первых N (где N - заданное число) принтеров с разрешенным доступом. Таблица 3 содержит список первых N (где N - заданное число) принтеров с запрещенным доступом. Эти таблицы включают следующие столбцы:

- **Device Name** - Имя принтера.
- **Access Count** - Количество запросов на доступ. Значения в этом столбце упорядочены по убыванию.

Top printed documents

Этот отчет показывает список наиболее часто печатаемых документов (файлов), отсортированный по количеству разрешенных и запрещенных попыток доступа:

- Группа 1 содержит как разрешенный, так и запрещенный доступ.
- Группа 2 содержит только разрешенный доступ.
- Группа 3 содержит только запрещенный доступ.

По умолчанию, отчет отображает первые 10 документов в каждой группе, но можно указать любое число документов.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.
- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.
- **Printer(s)** - Принтеры, выбранные для отчета.

Раздел “Результаты отчета” содержит три таблицы, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) документов с разрешенным и запрещенным доступом. Таблица 2 содержит список первых N (где N - заданное число) документов с разрешенным доступом. Таблица 3 содержит список первых N (где N - заданное число) документов с запрещенным доступом. Эти таблицы содержат следующие столбцы:

- **File Name** - Имя документа.
- **Access Count** - Количество запросов на доступ. Значения в этом столбце упорядочены по убыванию.

Top copied files by extension

Этот отчет содержит три группы наиболее часто копируемых расширений файлов исходя из количества запросов на доступ:

- Группа 1 содержит как разрешенный, так и запрещенный доступ.
- Группа 2 содержит только разрешенный доступ.
- Группа 3 содержит только запрещенный доступ.

По умолчанию, отчет отображает первые 10 расширений файлов в каждой группе, но можно указать любое число расширений.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **User(s)** - Пользователи, выбранные для отчета.
- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.

Раздел “Результаты отчета” содержит три таблицы и графики, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) расширений файлов с разрешенным и запрещенным доступом. Таблица 2 содержит список первых N (где N - заданное число) расширений файлов с разрешенным доступом. Таблица 3 содержит список первых N (где N - заданное число) расширений файлов с запрещенным доступом. Эти таблицы содержат следующие столбцы:

- **Extention** - Расширение файла.
- **Read** - Количество попыток чтения.
- **Write** - Количество попыток записи.

Таблицы также содержат строку **Total**, которая суммирует все значения в столбцах **Read** и **Write**.

Метка **No extension** применяется для всех файлов, для которых не задано расширение, метка **Other** применяется для файлов с прочими типами расширений, если процентное отношение совокупного множества таких файлов составляет менее 5% к общему количеству файлов. Метка **Direct access** применяется для всех операций прожига CD/DVD/BD и прямой записи на диск (например, операций форматирования диска).

Отчеты по данным журнала теневого копирования

Отчеты по данным журнала теневого копирования основаны на записях журнала теневого копирования (**Shadow Log**) сервера DeviceLock Enterprise Server. Все такие отчеты содержат объединенные данные, полученные из журнала теневого копирования и специального журнала записей, удаленных из журнала теневого копирования.

В этой категории предусмотрены следующие типы отчетов:

- Copied files per channel
- Top active computers
- Top active processes
- Top active users
- Top copied files
- Top copied files by extension
- Top printed documents

В консоли под каждым типом отчетов перечисляются задачи создания отчетов данного типа. Например, задачи создания отчетов Top active computers категории Audit Log перечисляются в узле консоли **DeviceLock Enterprise Server** > **Отчеты** > **Audit Log** > **Top active computers**. Если выбрать задачу в дереве консоли, на панели сведений отображается список отчетов, созданных этой задачей. Подробнее см. в разделе Задачи создания отчетов.

Copied files per channel

Этот отчет показывает статистику скопированных файлов по каналам передачи данных (устройства и/или протоколы), включая вложения электронной почты. Статистические сведения о скопированных файлах отсортированы по количеству скопированных файлов и общему размеру всех скопированных файлов (отдельно для разрешенных и запрещенных операций копирования).

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.
- **File Name** - Файлы, выбранные для отчета.
- **Channel(s)** - Каналы передачи данных, выбранные для отчета. Возможные варианты: **all devices** (все устройства), **all protocols** (все протоколы) и **all devices and protocols** (все устройства и протоколы).

Раздел “Результаты отчета” содержит четыре таблицы и четыре круговые диаграммы, которые представляют обработанные данные в отчете. Таблица 1 показывает количество скопированных файлов по каждому каналу передачи данных для разрешенных операций копирования. Таблица 2 показывает количество скопированных файлов по каждому каналу передачи данных для запрещенных операций копирования. Таблицы 1 и 2 содержат следующие столбцы:

- **Channel** - Канал передачи данных.
- **Number of Files** - Количество скопированных файлов.

Таблицы 1 и 2 также содержат строку **Total**, которая суммирует все значения в столбце **Number of Files**.

Таблица 3 показывает общий размер скопированных файлов по каждому каналу передачи данных для разрешенных операций копирования. Таблица 4 показывает общий размер скопированных файлов по каждому каналу передачи данных для запрещенных операций копирования.

Таблицы 3 и 4 содержат следующие столбцы:

- **Channel** - Канал передачи данных.
- **Data Size** - Общий размер всех скопированных файлов.

Таблицы 3 и 4 также содержат строку **Total**, которая суммирует все значения в столбце **Data Size**.

К каждой таблице прилагается круговая диаграмма, которая отображает данные в виде процентных долей.

Top active computers

Этот отчет показывает список наиболее активно используемых компьютеров, отсортированный по количеству скопированных файлов и общему размеру скопированных файлов. По умолчанию, отчет отображает первые 10 компьютеров, но можно указать любое число компьютеров.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.
- *Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.*
- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.
- **File Name** - Файлы, выбранные для отчета.

Раздел “Результаты отчета” содержит шесть таблиц, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) компьютеров с разрешенным и запрещенным доступом по количеству скопированных файлов. Таблица 2 содержит список первых N (где N - заданное число) компьютеров с разрешенным и запрещенным доступом по объему скопированных данных. Таблица 3 содержит список первых N (где N - заданное число) компьютеров с разрешенным доступом по количеству скопированных файлов. Таблица 4 содержит список первых N (где N - заданное число) компьютеров с разрешенным доступом по объему скопированных данных. Таблица 5 содержит список первых N (где N - заданное число) компьютеров с запрещенным доступом по количеству скопированных файлов. Таблица 6 содержит список первых N (где N - заданное число) компьютеров с запрещенным доступом по объему скопированных данных.

Таблицы 1, 3 и 5 содержат следующие столбцы:

- **Computer Name** - Имя компьютера.
- **Access Count** - Количество запросов на доступ. Значения в этом столбце упорядочены по убыванию.

Таблицы 2, 4 и 6 содержат следующие столбцы:

- **Computer Name** - Имя компьютера.
- **Data Size** - Общий размер всех скопированных файлов. Значения в этом столбце упорядочены по убыванию.

Top active processes

Этот отчет показывает список наиболее активных процессов (приложений), отсортированный по количеству скопированных файлов и общему размеру скопированных файлов. По умолчанию, отчет отображает первые 10 процессов, но можно указать любое число процессов.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.
- **File Name** - Файлы, выбранные для отчета.

Раздел “Результаты отчета” содержит шесть таблиц, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) процессов с разрешенным и запрещенным доступом по количеству скопированных файлов. Таблица 2 содержит список первых N (где N - заданное число) процессов с разрешенным и запрещенным доступом по объему скопированных данных. Таблица 3 содержит список первых N (где N - заданное число) процессов с разрешенным доступом по количеству скопированных файлов. Таблица 4 содержит список первых N (где N - заданное число) процессов с разрешенным доступом по объему скопированных данных. Таблица 5 содержит список первых N (где N - заданное число) процессов с запрещенным доступом по количеству скопированных файлов. Таблица 6 содержит список первых N (где N - заданное число) процессов с запрещенным доступом по объему скопированных данных.

Таблицы 1, 3 и 5 содержат следующие столбцы:

- **Process Name** - Имя процесса.
- **Access Count** - Количество запросов на доступ. Значения в этом столбце упорядочены по убыванию.

Таблицы 2, 4 и 6 содержат следующие столбцы:

- **Process Name** - Имя процесса.
- **Data Size** - Общий размер всех скопированных файлов. Значения в этом столбце упорядочены по убыванию.

Top active users

Этот отчет показывает список наиболее активных пользователей, отсортированный по количеству скопированных файлов и общему размеру скопированных файлов. По умолчанию, отчет отображает первые 10 пользователей, но можно указать любое число пользователей.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.
- **File Name** - Файлы, выбранные для отчета.

Раздел “Результаты отчета” содержит шесть таблиц, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) пользователей с разрешенным и запрещенным доступом по количеству скопированных файлов. Таблица 2 содержит список первых N (где N - заданное число) пользователей с разрешенным и запрещенным доступом по объему скопированных данных. Таблица 3 содержит список первых N (где N - заданное число) пользователей с разрешенным доступом по количеству скопированных файлов. Таблица 4 содержит список первых N (где N - заданное число) пользователей с разрешенным доступом по объему скопированных данных. Таблица 5 содержит список первых N (где N - заданное число) пользователей с запрещенным доступом по количеству скопированных файлов. Таблица 6 содержит список первых N (где N - заданное число) пользователей с запрещенным доступом по объему скопированных данных.

Таблицы 1, 3 и 5 содержат следующие столбцы:

- **User Name** - Имя пользователя.
- **Access Count** - Количество запросов на доступ. Значения в этом столбце упорядочены по убыванию.

Таблицы 2, 4 и 6 содержат следующие столбцы:

- **User Name** - Имя пользователя.
- **Data Size** - Общий размер всех скопированных файлов. Значения в этом столбце упорядочены по убыванию.

Top copied files

Этот отчет показывает список наиболее часто копируемых файлов, включая вложения электронной почты, отсортированный по числу скопированных файлов и общему размеру скопированных файлов. По умолчанию, отчет отображает первые 10 файлов, но можно указать любое число файлов.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.
- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.

Раздел “Результаты отчета” содержит шесть таблиц, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) скопированных файлов с разрешенным и запрещенным доступом по количеству копий. Таблица 2 содержит список первых N (где N - заданное число) скопированных файлов с разрешенным и запрещенным доступом по размеру. Таблица 3 содержит список первых N (где N - заданное число) скопированных файлов с разрешенным доступом по количеству копий. Таблица 4 содержит список первых N (где N - заданное число) скопированных файлов с разрешенным доступом по размеру. Таблица 5 содержит список первых N (где N - заданное число) скопированных файлов с запрещенным доступом по количеству копий. Таблица 6 содержит список первых N (где N - заданное число) скопированных файлов с запрещенным доступом по размеру.

Таблицы 1, 3 и 5 содержат следующие столбцы:

- **File Name** - Имя файла.
- **Number of Files** - Количество скопированных файлов. Значения в этом столбце упорядочены по убыванию.

Таблицы 2, 4 и 6 содержат следующие столбцы:

- **File Name** - Имя файла.
- **Data Size** - Общий размер всех скопированных файлов. Значения в этом столбце упорядочены по убыванию.

Top copied files by extension

Этот отчет показывает список наиболее часто копируемых расширений файлов, отсортированный по числу скопированных файлов, включая вложения электронной почты и общему размеру скопированных файлов. По умолчанию, отчет отображает первые 10 расширений файлов, но можно указать любое число расширений.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.
- **Channel(s)** - Типы устройств и/или протоколы, выбранные для отчета.

Раздел “Результаты отчета” содержит шесть таблиц, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) скопированных расширений файлов с разрешенным и запрещенным доступом по количеству копий. Таблица 2 содержит список первых N (где N - заданное число) скопированных расширений файлов с разрешенным и запрещенным доступом по размеру. Таблица 3 содержит список первых N (где N - заданное число) скопированных расширений файлов с разрешенным доступом по количеству копий. Таблица 4 содержит список первых N (где N - заданное число) скопированных расширений файлов с разрешенным доступом по размеру. Таблица 5 содержит список первых N (где N - заданное число) скопированных расширений файлов с запрещенным доступом по количеству копий. Таблица 6 содержит список первых N (где N - заданное число) скопированных расширений файлов с запрещенным доступом по размеру.

Таблицы 1, 3 и 5 содержат следующие столбцы:

- **Extension** - Расширение файла.
- **Number of Files** - Количество скопированных файлов. Значения в этом столбце упорядочены по убыванию.

Таблицы 1, 3 и 5 также содержат строку **Total**, которая суммирует все значения в столбце **Number of Files**.

Таблицы 2, 4 и 6 содержат следующие столбцы:

- **Extension** - Расширение файла.
- **Data Size** - Общий размер всех скопированных файлов. Значения в этом столбце упорядочены по убыванию.

Таблицы 2, 4 и 6 также содержат строку **Total**, которая суммирует все значения в столбце Data Size.

К каждой таблице прилагается круговая диаграмма, которая отображает данные в виде процентных долей.

Метка **No extension** применяется для всех файлов, для которых не задано расширение, метка **Other** применяется для файлов с прочими типами расширений, если процентное отношение совокупного множества таких файлов составляет менее 5% к общему количеству файлов. Метка **Direct access** применяется для всех операций прожига CD/DVD/BD и прямой записи на диск (например, операций форматирования диска).

Top printed documents

Этот отчет показывает список наиболее часто печатаемых документов (файлов), отсортированный по числу напечатанных файлов и общему размеру напечатанных файлов. По умолчанию, отчет отображает первые 10 документов, но можно указать любое число документов.

Отчет состоит из трех разделов - “Заголовок отчета”, “Параметры отчета” и “Результаты отчета”.

В разделе “Заголовок отчета” приводится название типа отчета.

В разделе “Параметры отчета” предоставляется следующая информация о параметрах отчета, заданных при его формировании:

- **Period** - Начальная и конечная дата и время диапазона записей журнала, включенных в отчет в соответствии с настройкой Отчетный период в задаче создания отчета.

  Формат даты/времени в полях “Period from” и “to” определяется форматом даты/времени для учетной записи пользователя, под которой работает DeviceLock Enterprise Server.

- **Computer(s)** - Компьютеры, выбранные для отчета.
- **Users(s)** - Пользователи, выбранные для отчета.
- **Printer(s)** - Принтеры, выбранные для отчета.

Раздел “Результаты отчета” содержит шесть таблиц, которые представляют обработанные данные в отчете. Таблица 1 содержит список первых N (где N - заданное число) напечатанных файлов с разрешенным и запрещенным доступом по количеству копий. Таблица 2 содержит список первых N (где N - заданное число) напечатанных файлов с разрешенным и запрещенным доступом по размеру. Таблица 3 содержит список первых N (где N - заданное число) напечатанных файлов с разрешенным доступом по количеству копий. Таблица 4 содержит список первых N (где N - заданное число) напечатанных файлов с разрешенным доступом по размеру. Таблица 5 содержит список первых N (где N - заданное число) напечатанных файлов с запрещенным доступом по количеству копий. Таблица 6 содержит список первых N (где N - заданное число) напечатанных файлов с запрещенным доступом по размеру.

Таблицы 1, 3 и 5 содержат следующие столбцы:

- **File Name** - Имя документа.
- **Number of Files** - Количество напечатанных файлов. Значения в этом столбце упорядочены по убыванию.

Таблицы 2, 4 и 6 содержат следующие столбцы:

- **File Name** - Имя документа.
- **Data Size** - Общий размер всех напечатанных файлов. Значения в этом столбце упорядочены по убыванию.

Задачи создания отчетов

Для создания отчетов служат задачи, которые можно запускать на выполнение как вручную, так и по расписанию. При каждом выполнении задачи создается новый отчет в соответствии с параметрами данной задачи. В случае запуска задачи по расписанию сервер автоматически создает новые отчеты согласно настройкам расписания задачи.

Чтобы создать новую задачу, используйте команду **Создать задачу** из контекстного меню родительского узла в дереве консоли. Чтобы вручную создать новый отчет, используйте команду **Запустить задачу** из контекстного меню соответствующей задачи.

В консоли управления DeviceLock задачи группируются по категории и типу отчетов:

- Задачи создания графов связей перечисляются в узле **DeviceLock Enterprise Server** > **Отчеты** > **Граф связей**. Создание графа связей начните с выбора команды **Создать задачу** в контекстном меню узла **Граф связей**. Описание отчетов этой категории см. в разделе Графы связей.
- Задачи создания отчетов определенного типа из категории Audit Log перечисляются в узле, представляющем данный тип отчета под узлом **DeviceLock Enterprise Server** > **Отчеты** > **Audit Log** в дереве консоли. Создание отчета начните с выбора команды **Создать задачу** в контекстном меню типа отчета. Описание типов, представленных в этой категории, см. в разделе Отчеты по данным журнала аудита.
- Задачи создания отчетов определенного типа из категории Shadow Log перечисляются в узле, представляющем данный тип отчета под узлом **DeviceLock Enterprise Server** > **Отчеты** > **Shadow Log** в дереве консоли. Создание отчета начните с выбора команды **Создать задачу** в контекстном меню типа отчета. Описание типов, представленных в этой категории, см. в разделе Отчеты по данным журнала теневого копирования.

Для обновления информации в списке задач с учетом последних изменений используйте команду **Обновить** из контекстного меню соответствующего узла задач в дереве консоли или из контекстного меню любой задачи на панели сведений.

Если в дереве консоли выбрана задача создания отчетов, на панели сведений отображается список ее отчетов. Подробнее об этом списке см. в разделе Просмотр отчетов, созданных задачей.

Управление задачами предполагает:

- Создание задач
- Управление существующими задачами
- Просмотр отчетов, созданных задачей

Примечание: Когда несколько экземпляров DeviceLock Enterprise Server используют одну и ту же базу данных, задачи и отчеты, созданные на одном из них, можно просматривать и администрировать на любом из этих экземпляров сервера. Задача выполняется сервером, на котором она была создана или изменена в последний раз.

Создание задач

Для создания задачи требуется выполнить следующие действия:

1. Определить категорию и тип отчета, для которого необходимо создать задачу.

   Задача может создавать либо графы связей (см. Графы связей) либо отчеты определенного типа из категории Audit Log (см. Отчеты по данным журнала аудита) или Shadow Log (см. Отчеты по данным журнала теневого копирования).

2. Выполнить команду **Создать задачу** для соответствующей категории и типа отчетов:

   - Если требуется задача для создания графов связей, выберите команду из контекстного меню узла **DeviceLock Enterprise Server** > **Отчеты** > **Граф связей**.
   - Если требуется задача для создания отчетов определенного типа по данным журнала аудита, выберите команду из контекстного меню узла, представляющего данный тип отчета под узлом **DeviceLock Enterprise Server** > **Отчеты** > **Audit Log** в дереве консоли.
   - Если требуется задача для создания отчетов определенного типа по данным журнала теневого копирования, выберите команду из контекстного меню узла, представляющего данный тип отчета под узлом **DeviceLock Enterprise Server** > **Отчеты** > **Shadow Log** в дереве консоли.

3. Настроить параметры отчета в появившемся диалоговом окне (см. Диалоговое окно для настройки параметров отчета). Затем нажать кнопку **Далее**, чтобы перейти к настройке расписания и других параметров задачи.

4. Настроить расписание и другие параметры задачи в появившемся диалоговом окне (см. Диалоговое окно для настройки расписания и параметров задачи). Затем нажать кнопку **Готово** для завершения.

Диалоговое окно для настройки параметров отчета

Это диалоговое окно служит для просмотра или изменения параметров отчета. Оно появляется первым при настройке задачи создания отчета. Предоставляемые в нем параметры зависят от категории и типа отчетов, создаваемых задачей. Здесь описаны все возможные параметры отчета. В описании каждого параметра указывается, к каким отчетам применим этот параметр.

Все возможные параметры отчета:

- Отчетный период
- Контакты
- Включить внутренних пользователей
- Исключить внутренних пользователей
- Исключить внешние контакты
- Компьютер(ы)
- Версии
- Пользователи
- Имена файлов
- Принтер(ы)
- Порог
- Отчет об устройствах
- Трактовать ТС-устройства как обычные
- Отчет о протоколах
- Тип доступа
- Типы устройств
- Протокол(ы)
- Первые <число> компьютеров
- Первые <число> принтеров
- Первые <число> пользователей
- Первые <число> USB и FireWire устройств
- Первые <число> USB-устройств
- Первые <число> процессов
- Первые <число> файлов
- Первые <число> напечатанных документов

Отчетный период

Следующие параметры определяют временной промежуток для записей журнала, включаемых в отчет:

- **С** - В качестве начала промежутка можно выбрать дату самой ранней записи в журнале (опция **Первой записи**) или указать другую дату (опция **Записи от**). В отчет включаются только данные записей, выполненных не ранее указанной даты.
- **По** - В качестве конца промежутка можно выбрать самую позднюю дату самой поздней записи в журнале (опция **Последнюю запись**) или указать другую дату (опция **Записи от**). В отчет включаются только данные записей, выполненных не позднее указанной даты.
- **Последние** - Если вместо параметра **С** выбран параметр **Последние**, в отчет включаются только данные записей за определенное число дней, недель или месяцев до построения отчета. Необходимо указать желаемое число дней, недель или месяцев.

Контакты

Данный параметр задает список контактов для включения в отчет. Он имеется только у графа связей.

Контакт - это адрес электронной почты, идентификатор пользователя социальной сети или службы мгновенного обмена сообщениями и т.п. Контакты позволяют идентифицировать как пользователей, имеющих учетную запись в домене организации (внутренние пользователи), так и пользователей без такой учетной записи (внешние контакты).

На графе связей, у которого задан этот параметр, отображаются заданные контакты, а также пользователи, которые общались с этими контактами. При помощи такого графа связей легко выяснить, кто обменивается файлами и сообщениями с определенными лицами вне или внутри организации:

- Отображаются только пользователи, которые общались хотя бы с одним из заданных контактов, а также объекты, связанные с такими пользователями. Другие пользователи и связанные с ними объекты скрываются.
- Заданные контакты выделяются зеленым цветом и по умолчанию обводятся кружком.
- Для каждого из заданных контактов по умолчанию раскрываются следующие объекты:
    - Для внешнего контакта - объекты, связанные с пользователем, который наиболее активно общался с этим контактом.
    - Для контакта, принадлежащего внутреннему пользователю, - объекты, связанные с этим пользователем.

Таким образом граф связей помогает обнаруживать определенные контакты и выявлять их связи с пользователями.

Чтобы задать контакты для отображения в отчете, выполните одно из следующих действий:

- В поле **Контакты** введите имена или идентификаторы контактов, разделяя их точкой с запятой (;).

  В имени или идентификаторе контакта можно использовать знаки подстановки: звездочку (*) для обозначения любой последовательности символов, знак вопроса (?) для обозначения одного произвольного символа.

  - или -

- Нажмите кнопку **Загрузить**, чтобы импортировать контакты из текстового файла, в котором имя или идентификатор каждого контакта указаны в отдельной строке.

Включить внутренних пользователей

Этот параметр задает список внутренних пользователей для включения в отчет. Он имеется только у графа связей.

Внутренними являются пользователи внутри корпоративной сети и являющиеся членами домена организации.

Чтобы задать список внутренних пользователей для включения в отчет, выберите одну из следующих опций:

- **Все** - Опция, включенная по умолчанию. При выборе данной опции в отчет будут включены данные по всем пользователям, найденным в журналах DeviceLock.
- **Статический список** - Используется для задания статического неизменяемого списка пользователей. Чтобы задать статический список, после выбора пункта **Статический список** выполните следующие действия:
  1. Нажмите кнопку **Редактировать**, чтобы открыть диалоговое окно **Редактирование статического списка**.
  2. В диалоговом окне **Редактирование статического списка** выберите пользователей, используя следующие опции: **Active Directory**, **LDAP**, **Из файла**, **Вручную**, и затем используйте кнопки >, >>, <, << для добавления выбранных пользователей в список **Выбранные пользователи** или удаления пользователей из этого списка.

  Опция **Active Directory** позволяет выбрать пользователей из службы каталогов Active Directory. Щелкнув кнопку ..., можно задать имя пользователя и пароль для доступа к Active Directory.

  Опция **LDAP** позволяет выбрать пользователей из LDAP-совместимой службы каталогов. Щелкните кнопку ..., чтобы задать параметры соединения со службой каталогов.

  Опция **Из файла** позволяет импортировать список пользователей из текстового файла, и затем выбрать пользователей. Для открытия текстового файла со списком пользователей щелкните кнопку ... . Такой текстовый файл должен содержать одного пользователя на строку и может быть в кодировке Unicode или non-Unicode.

  Опция **Вручную** позволяет ввести имена пользователей вручную, печатая каждое имя на отдельной строке. Можно также щелкнуть кнопку ... и выбрать пользователей с помощью диалогового окна **Выбор: "Пользователи" или "Группы"**.

  Все выбранные пользователи отображаются в списке "Выбранные пользователи" в правой части диалогового окна.

  Для удаления отдельных пользователей из списка используйте кнопку со стрелкой влево < . Для массового добавления всех доступных имен пользователя или удаления всех выбранных пользователей за один раз используйте кнопки с двойными стрелками соответственно вправо >> или влево <<.

  Для задания имен пользователей можно также использовать знаки подстановки, такие как звездочка (*) и знак вопроса (?). Звездочка (*) заменяет любое количество символов. Знак вопроса (?) заменяет отдельный символ. Эти знаки подстановки можно использовать в любой части имени и в любом количестве.

- **Динамический список** - Данная опция позволяет настроить динамический список пользователей, который будет обновляться при каждом запуске создания отчета, так что пользователи будут добавляться в список или удаляться из списка по мере их добавления или удаления в выбранном контейнере службы каталогов. Для задания динамического списка пользователей, после выбора пункта **Динамический список** выполните следующие действия:

  1. Нажмите кнопку **Редактировать**, чтобы открыть диалоговое окно **Редактирование динамического списка**.
  2. В диалоговом окне **Редактирование динамического списка** выберите нужный контейнер в дереве AD или LDAP, затем нажмите кнопку **Выбрать**. Можно выбрать один или несколько контейнеров. Для включения в динамический список пользователей из контейнеров уровнем ниже выбранного, установите флаг **Просматривать вложенные контейнеры**. Для выполнения синхронизации с Active Directory установите флаг **Сихронизация**.

  Кнопка ... позволяет задать имя пользователя и пароль для доступа к AD (при выборе опции **Active Directory**) или параметры подключения к серверу LDAP-совместимой службы каталогов (при выборе опции **LDAP**).

Исключить внутренних пользователей

Этот параметр задает список внутренних пользователей, которые должны быть исключены из отчета. Он имеется только у графа связей.

Внутренними являются пользователи внутри корпоративной сети и являющиеся членами домена организации.

Чтобы задать список внутренних пользователей, не включаемых в отчет, выполните одно из следующих действий:

- В поле **Исключить внутренних пользователей** введите имена пользователей. Можно использовать знаки подстановки, такие как звездочка (*) и знак вопроса (?). Имена следует задавать в формате `<DomainName>\<UserName>`. По умолчанию это поле содержит `NT Authority\*`, чтобы исключить из отчета служебные учетные записи Windows, такие как Локальная служба (Local Service), Сетевая служба (Network Service) и Локальная система (Local System).

  Звездочка (*) заменяет любое количество символов. Знак вопроса (?) заменяет отдельный символ. Эти знаки подстановки можно использовать в любой части имени и в любом количестве. Для разделения имен пользователей используйте точку с запятой (;).

  - или -

- Нажмите кнопку **Обзор** для вызова диалогового окна **Выбор: "Пользователи"**. В диалоговом окне **Выбор: "Пользователи"** выполните следующее:

  - **Типы объектов** - Выберите желаемые типы объектов.
  - **Размещение** - Выберите папку, в которой следует искать объекты.
  - **Введите имена выбираемых объектов** - Введите имена объектов для поиска и выбора. Для разделения имен объектов используйте точку с запятой (;).
  - **Проверить имена** - Нажмите для поиска имен объектов, соответствующих заданным в поле **Введите имена выбираемых объектов**.
  - **Дополнительно** - Нажмите, чтобы использовать дополнительные возможности поиска объектов.

  - или -

- Нажмите кнопку **Загрузить** для импорта пользователей из текстового файла, где каждое имя указано в отдельной строке в формате <DomainName>\<UserName>.

Исключить внешние контакты

Этот параметр задает список внешних контактов, которые должны быть исключены из отчета. Он имеется только у графа связей.

Внешние контакты - это адреса электронной почты, идентификаторы социальных сетей и сервисов мгновенных сообщений, принадлежащие пользователям, которые находятся вне корпоративной сети и не являются членами домена организации.

Чтобы задать список внешних контактов, которые следует исключить из отчета, выполните одно из следующих действий:

- В поле **Включить внешние контакты** введите имена или идентификаторы контактов, разделяя их точкой с запятой (;).

  В имени или идентификаторе контакта можно использовать знаки подстановки: звездочку (*) для обозначения любой последовательности символов, знак вопроса (?) для обозначения любого отдельного символа.

  - или -

- Нажмите кнопку **Загрузить**, чтобы импортировать контакты из текстового файла, в котором имя или идентификатор каждого контакта указаны в отдельной строке.

Компьютер(ы)

Этот параметр определяет компьютеры для отчета. Он имеется у всех отчетов, за исключением Top active computers и графа связей.

По умолчанию поле **Компьютер(ы)** не заполнено. Это означает, что в отчет будут включены данные по всем компьютерам, фигурирующим в базе данных DeviceLock Enterprise Server.

Чтобы указать компьютеры для отчета, выполните следующее:

- В поле **Компьютер(ы)** введите имена компьютеров с использованием подстановочных символов, таких как звездочка (*) и знак вопроса (?). Например, если ввести ***.mydomain.com**, то в отчет будут включены данные по всем компьютерам в домене mydomain.com.

  Звездочка (*) заменяет любое количество символов. Знак вопроса (?) заменяет отдельный символ. Эти знаки подстановки можно использовать в любой части имени и в любом количестве. Если компьютеров несколько, их следует разделять запятой (,) или точкой с запятой (;).

  - или -

- Нажмите кнопку **Обзор** рядом с полем **Компьютер(ы)**, а затем используйте один из следующих вариантов выбора компьютеров в появившемся диалоговом окне **Редактирование статического списка**:

  - **Active Directory** - Этот вариант выбран по умолчанию. Он позволяет выбрать компьютеры из службы каталогов Active Directory следующим образом:

    a) Нажмите кнопку ..., чтобы указать дополнительные учетные данные для доступа в Active Directory. Для получения дополнительной информации см. описание учетных данных Active Directory.

    b) В левой части диалогового окна **Редактирование статического списка** установите флажки рядом с нужными компьютерами.

    c) Нажмите кнопку с одной стрелкой, направленной вправо: >.

    Выбранные компьютеры отображаются в области "Выбранные компьютеры" в правой части диалогового окна.

    Чтобы удалить отдельные компьютеры из списка выбранных компьютеров, используйте кнопку с одной стрелкой, направленной влево: <.

    Чтобы добавить или удалить все доступные компьютеры из списка выбранных компьютеров одновременно, используйте кнопку >> *или* <<.

- **Из БД** - Компьютеры можно выбрать из базы данных сервера DeviceLock Enterprise Server, которая показывает все компьютеры, с которых сервер когда-либо получал данные аудита и теневого копирования. Если выбран этот вариант:

  a) В левой части диалогового окна **Редактирование статического списка** установите флажки рядом с нужными компьютерами.

  b) Нажмите кнопку с одной стрелкой, направленной вправо: >.

     Выбранные компьютеры отображаются в области "Выбранные компьютеры" в правой части диалогового окна.

     Чтобы удалить отдельные компьютеры из списка выбранных компьютеров, используйте кнопку с одной стрелкой, направленной влево: <.

     Чтобы добавить или удалить все доступные компьютеры из списка выбранных компьютеров одновременно, используйте кнопку >> *или* <<.

- **LDAP** - Компьютеры можно выбрать из LDAP-совместимой службы каталогов. Если выбрана этот вариант:

  a) Нажмите кнопку ..., чтобы открыть диалоговое окно **Настройки LDAP** и указать дополнительные учетные данные для доступа к LDAP-серверу. Для получения дополнительной информации см. описание параметров LDAP.

  b) В левой части диалогового окна **Редактирование статического списка** установите флажки рядом с нужными компьютерами.

  c) Нажмите кнопку с одной стрелкой, направленной вправо: >.

     Выбранные компьютеры отображаются в области "Выбранные компьютеры" в правой части диалогового окна.

     Чтобы удалить отдельные компьютеры из списка выбранных компьютеров, используйте кнопку с одной стрелкой, направленной влево: <.

     Чтобы добавить или удалить все доступные компьютеры из списка выбранных компьютеров одновременно, используйте кнопку >> *или* <<.

- **Из файла** - Компьютеры можно выбрать из внешнего текстового файла. Текстовый файл должен содержать имена или IP-адреса компьютеров, каждое из которых должно быть записано на отдельной строке в Юникоде или не в Юникоде. Если выбрана этот вариант:

  a) Нажмите кнопку ..., чтобы выбрать текстовый файл со списком компьютеров.

  b) В появившемся диалоговом окне найдите и откройте требуемый файл.

     Имена компьютеров, содержащиеся в файле, отображаются в левой части диалогового окна "Редактирование статического списка".

  c) В левой части диалогового окна **Редактирование статического списка** выберите нужные компьютеры, а затем нажмите кнопку >.

     Выбранные компьютеры отображаются в области "Выбранные компьютеры" в правой части диалогового окна.

     Чтобы удалить отдельные компьютеры из списка выбранных компьютеров, используйте кнопку с одной стрелкой, направленной влево: <.

     Чтобы добавить или удалить все доступные компьютеры из списка выбранных компьютеров одновременно, используйте кнопку >> *или* <<.

- **Вручную** - Компьютеры для отчета можно задать вручную. Если выбран этот вариант:

  a) В левой части диалогового окна **Редактирование статического списка** введите имена компьютеров или их IP-адреса. После ввода каждого имени компьютера нажимайте клавишу ENTER, чтобы каждое имя компьютера находилось на отдельной строке.

  b) В левой части диалогового окна **Редактирование статического списка** выберите нужные компьютеры, а затем нажмите кнопку `>`.

  Выбранные компьютеры отображаются в области "Выбранные компьютеры" в правой части диалогового окна.

  Чтобы удалить отдельные компьютеры из списка выбранных компьютеров, используйте кнопку с одной стрелкой, направленной влево: `<`.

  Чтобы добавить или удалить все доступные компьютеры из списка выбранных компьютеров одновременно, используйте кнопку `>>` *или* `<<`.

Версии

Этот параметр задает версии сервиса DeviceLock для отчета. Он имеется только у отчетов DeviceLock Service versions и DeviceLock Service versions by computers.

По умолчанию поле **Версии** не заполнено. Это означает, что в отчет будут включены данные по всем компьютерам, на которых установлен сервис DeviceLock, фигурирующим в базе данных сервера DeviceLock Enterprise Server.

Чтобы указать версии для отчета, введите в поле **Версии** номера версий с использованием подстановочных символов, таких как звездочка (*) и знак вопроса (?). Например, введите 6.4.?, чтобы указать все версии 6.4.x.

Звездочка (*) заменяет любое количество символов. Знак вопроса (?) заменяет отдельный символ. Эти знаки подстановки можно использовать в любой части имени и в любом количестве. Если версий несколько, их следует разделять запятой (,) или точкой с запятой (;).

Пользователи

Этот параметр определяет пользователей для отчета. Он имеется у всех отчетов, за исключением Top active computers, Top active processes и Top active users, а также графа связей.

По умолчанию поле **Пользователи** не заполнено. Это означает, что отчет будет содержать данные по всем пользователям, фигурирующим в базе данных сервера DeviceLock Enterprise Server.

Чтобы указать пользователей для отчета, выполните следующее:

- В поле **Пользователи** введите имена пользователей с использованием подстановочных символов, таких как звездочка (*) и знак вопроса (?). Например, если ввести `mydomain*`, то в отчет будут включены данные по всем пользователям в домене mydomain.

  Звездочка (*) заменяет любое количество символов. Знак вопроса (?) заменяет отдельный символ. Эти знаки подстановки можно использовать в любой части имени и в любом количестве. Если пользователей несколько, их следует разделять запятой (,) или точкой с запятой (;).

  Примечание: В поле **Пользователи** нельзя указывать группы пользователей.

  - или -

- Нажмите кнопку **Обзор** рядом с полем **Пользователи**, а затем выполните следующее:

  a) В поле **Введите имена выбираемых объектов** открывшегося диалогового окна **Выбор: "Пользователи"** введите имена пользователей через точку с запятой (;).

  b) Нажмите кнопку **OK**.

Имена файлов

Этот параметр указывает файлы для отчета. Он имеется только у отчетов Top active users, Top active computers, Top active processes, Copied files per channel и Copied files per channel из категории Shadow Log.

По умолчанию поле **Имена файлов** не заполнено. Это означает, что в отчет будут включены данные по всем файлам, фигурирующим в базе данных сервера DeviceLock Enterprise Server.

Чтобы указать файлы для отчета, введите в это поле имена файлов с использованием подстановочных символов, таких как звездочка (*) и знак вопроса (?). Например, если ввести ***.txt**, то в отчет будут включены данные по всем файлам с расширением .txt. Еще один пример: чтобы указать все файлы, имена которых начинаются с любых букв или знаков, содержат слово “price” и имеют любое расширение, введите ***price*.***

Звездочка (*) заменяет любое количество символов. Знак вопроса (?) заменяет отдельный символ. Эти знаки подстановки можно использовать в любой части имени и в любом количестве. Если файлов несколько, их следует разделять запятой (,) или точкой с запятой (;).

Принтер(ы)

Этот параметр указывает имена принтеров для отчета. Он имеется только у отчетов Top printed documents.

По умолчанию поле **Принтер(ы)** не заполнено. Это означает, что в отчет будут включены данные по всем принтерам, фигурирующим в базе данных сервера DeviceLock Enterprise Server.

Чтобы задать принтеры для отчета, введите в это поле имена принтеров с использованием подстановочных символов, таких как звездочка (*) и знак вопроса (?). Например, если ввести PDF*, то в отчет будут включены данные по всем принтерам, имена которых начинаются с PDF.

Звездочка (*) заменяет любое количество символов. Знак вопроса (?) заменяет отдельный символ. Эти знаки подстановки можно использовать в любой части имени и в любом количестве. Если файлов несколько, их следует разделять запятой (,) или точкой с запятой (;).

Порог

Этот параметр задает интервал времени (в секундах) между событиями, зарегистрированными в журнале, и используется для объединения событий. Он имеется у всех отчетов из категории Audit Log, за исключением отчетов Top inserted USB & FireWire devices.

Учитывая, что каждое действие пользователя порождает множество событий, для построения отчетов DeviceLock использует принцип объединения событий, зафиксированных в журнале аудита. DeviceLock сравнивает время события со временем последующих событий. Если разница во времени событий меньше или равна значению **Порог**, события одного типа (разрешенные попытки доступа или запрещенные попытки доступа) объединяются в одно совокупное событие, если верны все следующие условия:

- События регистрируются для одного и того же компьютера.
- События регистрируются для одного и того же типа устройств или протокола.

Отчет об устройствах

Установите флажок **Отчет об устройствах**, чтобы включить в отчет данные по всем типам устройств. Если этот флажок не установлен, информация по событиям, связанным с устройствами, не будет включена в отчет. Этот флажок доступен только для отчетов Allowed & Denied access requests per channel, Allowed vs. Denied access requests и Copied files per channel.

Трактовать ТС-устройства как обычные

Установите флажок **Трактовать ТС-устройства как обычные**, чтобы данные по использованию ТС-устройств подсчитывались в отчете вместе с данными для обычных устройств:

- ТС-устройства (Подключенные диски) - относить к типу **Съемные устройства**
- ТС-устройства (Последовательный порт) - относить к типу **Последовательный порт**
- ТС-устройства (USB-порт) - относить к типу **USB-порт**
- ТС-устройства (Буфер обмена) - относить к типу **Буфер обмена**

Если этот флажок не установлен, данные для ТС-устройств будут подсчитываться и отображаться отдельно. Этот флажок доступен только для отчетов Allowed & Denied access requests per channel, Read & Write access requests per device type и Copied files per channel.

Отчет о протоколах

Установите флажок **Отчет о протоколах**, чтобы включить в отчет данные по всем сетевым протоколам. Если этот флажок не установлен, информация по событиям, связанным с сетевыми протоколами, не будет включена в отчет. Этот флажок доступен только для отчетов Allowed & Denied access requests per channel, Allowed vs. Denied access requests и Copied files per channel.

Тип доступа

Этот параметр определяет тип событий, которые будут включаться в отчет. Он имеется только у отчетов Read & Write access requests per devicee type из категории Audit Log.

Установите флажок **Разрешено** для включения в отчет записей об успешных попытках доступа. Установите флажок **Запрещено** для включения в отчет записей о запрещенных попытках доступа. Эти флажки можно устанавливать вместе или по отдельности.

Типы устройств

Этот параметр определяет типы устройств для включения в отчет. Он имеется только у отчетов Top active computers, Top active users, Top copied files, Top active processes и Top copied files by extension.

Чтобы определить типы устройств для отчета, установите флажки рядом с необходимыми типами устройств.

Протокол(ы)

Этот параметр определяет сетевые протоколы для включения в отчет. Он имеется у графа связей, а также у отчетов Top active computers, Top active users, Top copied files, Top active processes и Top copied files by extension.

Чтобы определить сетевые протоколы для отчета, установите флажки рядом с необходимыми протоколами.

Примечание:

- Если оба параметра - **Типы устройств** и **Протокол(ы)** - не выбраны, отчет будет содержать данные по всем типам устройств и всем сетевым протоколам. Если выбран любой из этих параметров и указаны типы устройств и протоколы, отчет будет содержать данные только для указанных типов устройств и протоколов.
- Имеется возможность выбрать условный сетевой протокол **Другие**, включающий в себя все данные, переданные по нераспознанным протоколам и подпавшие под правила аудита белого списка протоколов (протоколы **Любой** и **SSL**) и IP-файрвола.
- Если выбран протокол **Другие** и действует настройка безопасности **Блокировать трафик Tor-браузера**, в отчете учитывается количество попыток использовать Tor-браузер, которые расцениваются как запрещенные попытки доступа к этому протоколу.

Первые <число> компьютеров

Этот параметр определяет количество наиболее часто используемых компьютеров для включения в отчет. Он имеется только у отчета Top active computers.

Значение по умолчанию - 10. Чтобы изменить значение по умолчанию, установите требуемое число в поле **Первые** <*число*> **компьютеров**.

Первые <число> принтеров

Этот параметр определяет количество наиболее часто используемых принтеров для включения в отчет. Он имеется только у отчета Top used Printers.

Значение по умолчанию - 10. Чтобы изменить значение по умолчанию, установите требуемое число в поле **Первые** <*число*> **принтеров**.

Первые <число> пользователей

Этот параметр определяет количество наиболее активных пользователей для включения в отчет. Он имеется только у отчета Top active users.

Значение по умолчанию - 10. Чтобы изменить значение по умолчанию, установите требуемое число в поле **Первые** <*число*> **пользователей**.

Первые <число> USB и FireWire устройств

Этот параметр определяет количество наиболее часто подключаемых USB и FireWire устройств для включения в отчет. Он имеется только у отчета Top inserted USB & FireWire devices.

Значение по умолчанию - 10. Чтобы изменить значение по умолчанию, установите требуемое число в поле **Первые** <*число*> **USB и FireWire устройств**.

Первые <число> USB-устройств

Этот параметр определяет количество наиболее часто используемых USB устройств для включения в отчет. Он имеется только у отчета Top used USB devices.

Значение по умолчанию - 10. Чтобы изменить значение по умолчанию, установите требуемое число в поле **Первые** <*число*> **USB-устройств**.

Первые <число> процессов

Этот параметр определяет количество наиболее активных процессов для включения в отчет. Он имеется только у отчета Top active processes.

Значение по умолчанию - 10. Чтобы изменить значение по умолчанию, установите требуемое число в поле **Первые** <*число*> **процессов**.

Первые <число> файлов

Этот параметр определяет количество наиболее часто копируемых файлов для включения в отчет. Он имеется только у отчета Top copied files и Top copied files by extension.

Значение по умолчанию - 10. Чтобы изменить значение по умолчанию, установите требуемое число в поле **Первые** <*число*> **файлов**.

Первые <число> напечатанных документов

Этот параметр определяет количество наиболее часто печатаемых документов для включения в отчет. Он имеется только у отчета Top printed documents.

Значение по умолчанию - 10. Чтобы изменить значение по умолчанию, установите требуемое число в поле **Первые** <*число*> **напечатанных документов**.

Диалоговое окно для настройки расписания и параметров задачи

Это диалоговое окно отображается вторым в серии диалоговых окон для настройки задач создания отчетов. После настройки параметров отчета это диалоговое окно можно использовать для просмотра или изменения расписания задачи и других параметров, в том числе:

- **Имя задачи** - Имя задачи не может быть пустым или состоять только из пробелов. У каждой задачи должно быть уникальное имя на сервере.
- **Активно** - Если этот флажок установлен, задача запускается автоматически по указанному расписанию.
- **Расписание** - Следующие параметры используются для настройки расписания:
  - **Однократно** - Однократный запуск. Укажите дату и время запуска задачи, или установите флажок **Запустить сейчас** для запуска задачи сразу после ее создания или изменения.
  - **Ежечасно** - Ежечасный запуск. Помимо даты и времени необходимо указать интервал запуска задачи. Например, значение 1 запускает задачу каждый час, а значение 2 - через час.
  - **Ежедневно** - Ежедневный запуск. Помимо даты и времени необходимо указать интервал запуска задачи. Например, значение 1 запускает задачу каждый день, а значение 2 - через день. Запуск задачи осуществляется ежедневно в соответствии с указанным временем.
  - **Еженедельно** - Еженедельный запуск. Помимо даты и времени необходимо указать интервал запуска задачи и дни недели, по которым задача будет запускаться. Например, значение 1 запускает задачу каждую неделю, а значение 2 - через неделю. Запуск задачи осуществляется в соответствии с указанным временем в каждый из указанных дней недели.
  - **Ежемесячно** - Ежемесячный запуск. Необходимо указать месяцы, недели месяца и дни недели для каждого месяца, по которым будет выполняться задача. Можно также настроить запуск задачи в определенный последний день недели каждого месяца.
- **Отправить отчет по e-mail** - Для доставки отчетов задачи по электронной почте установите этот флажок и заполните следующие поля:
  - **Получатели** - Укажите список электронных адресов получателей отчетов. Для разделения адресов в списке используйте точку с запятой (;).
  - **Формат отчета** - Выберите формат отправки отчетов данной задачи. Первоначально выбран формат, установленный по умолчанию (см. Выбор формата отчетов по умолчанию).

Примечание:

- Параметры отправки отчетов отсутствуют при настройке задачи создания графов связей, поскольку граф связей нельзя отправить по электронной почте.
- Для отправки отчетов необходимо указать почтовый сервер (см. Настройка электронной почты для доставки отчетов). Если почтовый сервер не указан, параметры отправки отчетов недоступны.

Управление существующими задачами

Когда в дереве консоли выбран узел **Граф связей** или какой-либо тип отчета, на панели сведений отображается список задач создания отчетов, со следующими сведениями по каждой задаче:

- **Имя** - Имя задачи.
- **Статус** - Одно из следующих значений:
  - **Ожидает** - Задача ждет следующего запуска по расписанию.
  - **Выполняется** - Задача выполняется.
  - **Закончена** - Последние выполнение задачи завершено успешно.
  - **Ошибка** - Последние выполнение задачи завершилось с ошибкой.
- **Расписание** - Расписание запуска задачи.
- **Время последнего запуска** - Дата и время последнего запуска данной задачи.

В контекстном меню задачи предоставляются следующие команды:

- **Редактировать задачу** - Просмотреть или изменить параметры задачи в диалоговых окнах, которые открывает эта команда.
- **Дублировать задачу** - Создать новую задачу путем копирования параметров выбранной задачи. Параметры новой задачи можно редактировать в диалоговых окнах, которые открывает эта команда.
- **Удалить задачу**/**Удалить задачи** - Удалить выбранную задачу или выбранные задачи. Несколько задач можно выбрать, используя клавишу `Shift` или `Ctrl`. При удалении задачи удаляются также все ее отчеты.
- **Запустить задачу**/**Запустить задачи** - Запустить выбранную задачу или задачи вручную независимо от расписания.
- **Остановить задачу** - Прекратить выполнение задачи, запущенной вручную.
- **Обновить** - Обновить список с учетом последних изменений.

Команды контекстного меню можно использовать для выполнения следующих действий:

- **Выполнить задачу** - Выберите команду **Запустить задачу**. Выполнение задачи приводит к созданию нового отчета. Команда **Запустить задачи** может использоваться для одновременного выполнения нескольких выбранных задач.
- **Просмотреть или изменить параметры отчета данной задачи** - Выберите команду **Редактировать задачу**, и затем просмотрите или измените параметры в появившемся диалоговом окне (см. Диалоговое окно для настройки параметров отчета). По завершении нажмите кнопку **Далее**, а затем **Готово**.
- **Просмотреть или изменить расписание и другие параметры задачи** - Выберите команду **Редактировать задачу**. Нажмите кнопку **Далее**, и затем просмотрите или измените параметры в появившемся диалоговом окне (см. Диалоговое окно для настройки расписания и параметров задачи). По завершении нажмите кнопку **Готово**.

  Диалоговые окна для редактирования задачи аналогичны используемым для создания задачи с единственным отличием, что при редактировании они отображают текущие значения параметров, позволяя изменять параметры выбранной задачи без создания новой.

- **Создать новую задачу путем копирования существующей задачи** - Выберите команду **Дублировать задачу** в контекстном меню задачи для копирования. Затем используйте диалоговые окна, отображаемые этой командой, чтобы просмотреть или изменить параметры новой задачи (см. Диалоговое окно для настройки параметров отчета, Диалоговое окно для настройки расписания и параметров задачи).

  Диалоговые окна для дублирования задачи аналогичны используемым для создания задачи с единственным отличием, что при дублировании они уже заполнены значениями параметров, скопированными из выбранной задачи.

- **Удалить некоторые задачи** - Выберите одну или несколько задач, щелкните эту выборку правой кнопкой мыши и нажмите **Удалить задачу** (если выбрана единственная задача) или **Удалить задачи** (если выбрано несколько задач). Чтобы выбрать несколько задач, используйте клавиши `Shift` или `Ctrl`. Задачу можно удалить, даже если у нее есть отчеты. В этом случае консоль запрашивает подтверждение, а затем удаляет задачу вместе со всеми ее отчетами, если пользователь консоли подтвердил удаление отчетов.

Просмотр отчетов, созданных задачей

Когда задача выбрана в дереве консоли, на панели сведений отображается список отчетов, созданных этой задачей, со следующими сведениями по каждому отчету:

- **Имя** - По умолчанию имя отчета состоит из имени задачи, за которым следуют дата и время запуска задачи.
- **Тип** - Возможные значения: **По расписанию** (задача была запущена по расписанию) или **Вручную** (задача была запущена вручную).
- **Статус** - Возможные значения:
  - **Создание** - Создание отчета продолжается.
  - **Готово** - Отчет успешно создан.
  - **Ошибка** - В отчете произошла ошибка. Щелкните этот статус для просмотра сообщения об ошибке. Для получения дополнительной информации об ошибке используйте Просмотрщик журнала сервера.
- **Отправлен** - Появляется только для отчетов категории Audit Log или Shadow Log. Возможные значения:
  - **Да** - Отчет, включенный в доставку по электронной почте, успешно доставлен всем или некоторым получателям. Значение **Да** отображается только после завершения процесса отправки.
  - **Нет** - Означает следующее:
    - Отчет не включен в доставку по электронной почте.

      - или -

    - Отчет, включенный в доставку по электронной почте, не был доставлен ни одному из указанных получателей.

  В случае ошибки при отправке отчета по электронной почте, определить причину можно путем просмотра записей в журнале сервера DeviceLock Enterprise Server (подробнее см. в разделе Просмотрщик журнала сервера).

  Если на вашем компьютере установлены и запущены программы защиты от вирусов и нежелательной почты, то в случае возникновения ошибки при отправке отчета по электронной почте информация об ошибке может не записываться в журнал сервера. Это происходит потому, что программы защиты от вирусов и нежелательной почты, например, Symantec Norton AntiVirus, могут автоматически перехватывать почтовые сообщения.

  Для получения дополнительной информации о работе программ защиты от вирусов и нежелательной почты обратитесь к документации производителя.

- **Запущен** - Дата и время начала создания отчета.
- **Закончен** - Дата и время завершения создания отчета.
- **Запущено** - Учетная запись, запустившая задачу создания данного отчета.
- **С компьютера** - Компьютер, с которого была запущена задача создания данного отчета.

В контекстном меню отчета на панели сведений предоставляются следующие команды:

- **Открыть** - Отобразить отчет.
- **Переименовать** - Изменить имя отчета.
- **Отправить отчет по e-mail** - Отправить готовый отчет по электронной почте. Введите адреса получателей отчета в диалоговом окне, которое появляется при выборе этой команды.
- **Сохранить как** - Экспортировать отчет в файл. Наведите указатель мыши на эту команду, чтобы выбрать формат экспорта.
- **Посмотреть параметры** - Открыть диалоговое окно для просмотра параметров данного отчета.
- **Удалить отчет**/**Удалить отчеты** - Удалить выбранный отчет или отчеты. Несколько отчетов можно выбрать, используя клавишу `Shift` или `Ctrl`.
- **Обновить** - Обновить список отчетов с учетом последних изменений.

Примечание:

- В меню для графа связей отсутствуют команды **Отправить отчет по e-mail** и **Сохранить как**, поскольку графы связей невозможно отправлять по электронной почте или сохранять в виде файлов.
- Для команды **Отправить отчет по e-mail** должен быть указан почтовый сервер (см. Настройка электронной почты для доставки отчетов). В противном случае эта команда не отображается в меню.

Подробнее о действиях по управлению отчетами см. в разделе Работа с отчетами.

Настройка электронной почты для доставки отчетов

DeviceLock может рассылать отчеты по электронной почте, используя для этого SMTP-сервер. Чтобы настроить доставку отчетов по электронной почте необходимо указать SMTP-сервер, через который будут отправляться отчеты, а также электронные адреса получателей отчетов.

Примечание: Графы связей и пользовательские досье не могут рассылаться по электронной почте.

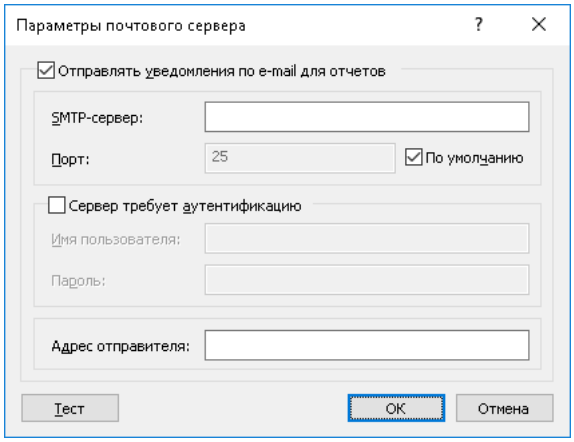
Чтобы настроить доставку отчетов по электронной почте

1. Откройте консоль DeviceLock Management Console и подключитесь к компьютеру, на котором работает DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** щелкните правой кнопкой мыши **Отчеты**, а затем выберите команду **Настройки уведомления**.

   - или -

   Выберите **Отчеты**, а затем щелкните значок **Настройки уведомления** на панели инструментов.

   Появится диалоговое окно "Параметры почтового сервера".



4. Заполните диалоговое окно **Параметры почтового сервера** следующим образом:
   - **Отправлять уведомления по e-mail для отчетов** - Чтобы включить доставку отчетов по электронной почте, установите этот флажок и введите параметры сервера электронной почты (SMTP) в соответствующие поля диалогового окна.

     Снимите флажок **Отправлять уведомления по e-mail для отчетов**, если требуется отключить доставку отчетов по электронной почте.
   - **SMTP-сервер** - Укажите SMTP-сервер для отправки отчетов. Введите в этом поле имя или IP-адрес сервера.
   - **Порт** - Укажите порт для подключения к SMTP-серверу. Порт по умолчанию - 25. Снимите флажок **По умолчанию**, если требуется ввести другой номер порта.

     Примечание: DeviceLock поддерживает как незащищенные, так и защищенные (SSL) подключения к SMTP-серверу. Тип подключения устанавливается автоматически, в зависимости от того, включен ли SSL на SMTP-сервере.

- **Сервер требует аутентификацию** - Установите этот флажок, если для подключения к указанному SMTP-серверу требуется аутентификация. Снимите этот флажок, если аутентификация не требуется.

  Если флажок **Сервер требует аутентификацию** установлен, в поле **Имя пользователя** и **Пароль** необходимо указать имя и пароль учетной записи электронной почты, у которой есть разрешение на подключение к SMTP-серверу.

- **Адрес отправителя** - Укажите адрес для отображения в поле **От** сообщений электронной почты с отчетами DeviceLock.

5. Для проверки заданных параметров почтового сервера нажмите кнопку **Тест**.
6. В диалоговом окне, которое открывается по нажатию кнопки **Тест**, укажите электронный адрес получателя и нажмите кнопку **OK** для отправки тестового письма.

   Если параметры почтового сервера указаны правильно, письмо будет доставлено получателю. В противном случае консоль отобразит сообщение с описанием проблемы.
7. По завершении нажмите кнопку **OK**.

Выбор формата отчетов по умолчанию

Вы можете выбрать выходной формат отчетов, который будет использоваться по умолчанию. Возможные варианты:

- Формат HTML (*.htm)
- Формат PDF (*.pdf)
- Формат Rich Text Format (*.rtf)

По умолчанию DeviceLock использует формат PDF для отчетов.

Чтобы выбрать выходной формат отчетов по умолчанию

1. Откройте консоль DeviceLock Management Console и подключитесь к компьютеру, на котором работает DeviceLock Enterprise Server.
2. В дереве консоли раскройте узел **DeviceLock Enterprise Server**.
3. В узле **DeviceLock Enterprise Server** щелкните правой кнопкой мыши **Отчеты**, укажите на пункт меню **Установить формат по умолчанию**, а затем выберите один из следующих вариантов: **HTML**, **PDF** или **RTF**.

Примечание: Выбор формата отчетов не влияет на графы связей и пользовательские досье.

Работа с отчетами

В этом разделе приводятся краткие инструкции по выполнению следующих операций:

- Создание отчетов
- Обновление списков отчетов
- Просмотр отчетов
- Просмотр параметров отчета
- Экспорт и сохранение отчетов
- Отправка отчетов по электронной почте
- Удаление отчетов

Внимание: Данные инструкции не относятся к пользовательским досье.

Создание отчетов

Для создания отчетов используются задачи, которые можно запускать как по расписанию, так и вручную. При каждом запуске задачи создается новый отчет. Подробнее см. в разделе Задачи создания отчетов.

Чтобы создать отчет

1. Откройте консоль DeviceLock Management Console и подключитесь к серверу DeviceLock Enterprise Server.
2. В дереве консоли в разделе **DeviceLock Enterprise Server** > **Отчеты** найдите задачу для создания требуемого отчета.

   Создайте задачу, если ее еще нет на сервере. Инструкции см. в разделе Создание задач.
3. Выполните одно из следующих действий:
   - Чтобы сразу создать отчет, щелкните задачу правой кнопкой мыши и выберите команду **Запустить задачу**.
   - Чтобы создать отчет по расписанию, щелкните задачу правой кнопкой мыши, выберите команду **Редактировать задачу** и перейдите к диалоговому окну для настройки расписания. Просмотрите или измените расписание задачи в этом диалоговом окне (см. Диалоговое окно для настройки расписания и параметров задачи).

Для просмотра результатов создания отчета, выберите задачу в дереве консоли. Информация об отчетах отображается на панели сведений (см. Просмотр отчетов, созданных задачей).

Обновление списков отчетов

Если в дереве консоли выбрана задача создания отчетов, на панели сведений отображается список отчетов, созданных этой задачей. Поскольку консоль не обновляет этот список автоматически, его обновление требуется выполнять вручную.

Чтобы обновить список отчетов

1. Откройте консоль DeviceLock Management Console и подключитесь к серверу DeviceLock Enterprise Server.
2. В дереве консоли в разделе **DeviceLock Enterprise Server** > **Отчеты** найдите задачу создания требуемых отчетов.
3. Выполните одно из следующих действий:
   - Щелкните задачу правой кнопкой мыши и выберите команду **Обновить** или выберите задачу и нажмите кнопку **Обновить** на панели инструментов.
   - Щелкните правой кнопкой мыши любой отчет в списке и выберите команду **Обновить** или выберите отчет в списке и нажмите кнопку **Обновить** на панели инструментов.

Просмотр отчетов

После успешного создания отчета его можно открыть и просмотреть в консоли DeviceLock Management Console.

Чтобы просмотреть отчет

1. Откройте консоль DeviceLock Management Console и подключитесь к серверу DeviceLock Enterprise Server.
2. В дереве консоли в разделе **DeviceLock Enterprise Server** > **Отчеты** найдите и выберите задачу, создавшую требуемый отчет.
3. В списке отчетов, который отображается на панели сведений, щелкните отчет правой кнопкой мыши и выберите команду **Открыть**.

Для просмотра графа связей можно также выбрать его под соответствующей задачей в дереве консоли.

Отчеты по данным журнала аудита или теневого копирования открываются в приложении, связанном с выбранным форматом отчетов по умолчанию. Обычно это Adobe Acrobat Reader, поскольку первоначально в качестве формата по умолчанию для отчетов выбран PDF. Acrobat Reader можно установить с веб-сайта компании Adobe по адресу get.adobe.com/reader.

Просмотр параметров отчета

Каждый отчет, созданный и хранящийся на сервере, содержит информацию о параметрах отчета, которые были установлены при его создании. Эти параметры можно просмотреть в консоли DeviceLock Management Console.

Чтобы просмотреть параметры отчета

1. Откройте консоль DeviceLock Management Console и подключитесь к серверу DeviceLock Enterprise Server.
2. В дереве консоли в разделе **DeviceLock Enterprise Server** > **Отчеты** найдите и выберите задачу, создавшую требуемый отчет.
3. В списке отчетов, который отображается на панели сведений, щелкните отчет правой кнопкой мыши и выберите команду **Посмотреть параметры**.

Значения параметров отображаются в диалоговом окне, аналогичном тому, что используется при создании задачи (см. Диалоговое окно для настройки параметров отчета).

Экспорт и сохранение отчетов

Отчеты, созданные и хранящиеся на сервере, могут быть экспортированы в файлы разных форматов (HTML, PDF или RTF) для сохранения локально или в сети.

Внимание: Графы связей невозможно экспортировать и сохранять в виде файлов, поскольку такие отчеты являются интерактивными.

Чтоб экспортировать и сохранить отчет

1. Откройте консоль DeviceLock Management Console и подключитесь к серверу DeviceLock Enterprise Server.
2. В дереве консоли в разделе **DeviceLock Enterprise Server** > **Отчеты** > **Audit Log** или **DeviceLock Enterprise Server** > **Отчеты** > **Shadow Log** найдите и выберите задачу, создавшую требуемый отчет.
3. В списке отчетов, который отображается на панели сведений, щелкните отчет правой кнопкой мыши, наведите указатель мыши на пункт меню **Сохранить как** и выберите желаемый формат экспорта: HTML, PDF или RTF.
4. В появившемся диалоговом окне выберите папку и укажите имя файла для хранения экспортированного отчета. Имя файла по умолчанию состоит из имени отчета, за которым следуют текущая дата и время.

Можно экспортировать и сохранить несколько отчетов одновременно:

1. Выбирайте отчеты в списке, удерживая нажатой клавишу `Shift` или `Ctrl`.
2. Щелкните выбранные отчеты правой кнопкой мыши, наведите указатель мыши на пункт меню **Сохранить как** и выберите желаемый формат экспорта: HTML, PDF или RTF.
3. В появившемся диалоговом окне выберите папку для экспортированных отчетов.

Примечание: Отчеты, экспортированные в формате HTML, сохраняются как .htm-файлы. Если исходный отчет содержит графические изображения, каждое изображение сохраняется как отдельный .gif-файл в папке, содержащей файл .htm.

Отправка отчетов по электронной почте

DeviceLock предоставляет следующие варианты отправки отчетов по электронной почте:

- У каждой задачи создания отчетов имеется параметр отправки результатов по электронной почте (см. Диалоговое окно для настройки расписания и параметров задачи). Если данный параметр включен, задача отправляет каждый вновь созданный отчет указанным получателям электронной почты.
- Консоль предоставляет команду для отправки готовых отчетов указанным получателям электронной почты.

Для отправки отчетов по электронной почте должен быть задан почтовый сервер. Подробнее о почтовом сервере см. в разделе Настройка электронной почты для доставки отчетов.

Внимание: Графы связей не могут быть отправлены по электронной почте, поскольку такие отчеты являются интерактивными.

Чтобы отправить готовый отчет по электронной почте

1. Откройте консоль DeviceLock Management Console и подключитесь к серверу DeviceLock Enterprise Server.
2. В дереве консоли в разделе **DeviceLock Enterprise Server** > **Отчеты** > **Audit Log** или **DeviceLock Enterprise Server** > **Отчеты** > **Shadow Log** найдите и выберите задачу, создавшую требуемый отчет.
3. В списке отчетов, который отображается на панели сведений, щелкните отчет правой кнопкой мыши и выберите команду **Отправить отчет по e-mail**.
4. В появившемся диалоговом окне введите адреса получателей электронной почты в следующем формате: `user@mailserver`. Разделяйте адреса запятой, точкой с запятой или пробелом.

Можно отправить несколько отчетов одновременно:

1. Выбирайте отчеты в списке, удерживая нажатой клавишу `Shift` или `Ctrl`.
2. Щелкните выбранные отчеты правой кнопкой мыши и выберите команду **Отправить отчет по e-mail**.
3. В появившемся диалоговом окне введите адреса получателей электронной почты.

Если при доставке отчета произошла ошибка, в журнале сервера записывается сообщение об ошибке. Для просмотра таких сообщений можно использовать Просмотрщик журнала сервера.

Примечание: Отчеты в формате HTML отправляются в теле сообщения, а не в виде вложений.

Удаление отчетов

В консоли управления DeviceLock имеется возможность удалять отчеты с сервера.

Чтобы удалить отчет

1. Откройте консоль DeviceLock Management Console и подключитесь к серверу DeviceLock Enterprise Server.
2. В дереве консоли в разделе **DeviceLock Enterprise Server** > **Отчеты** найдите и выберите задачу, создавшую отчет, который требуется удалить.
3. В списке отчетов, который отображается на панели сведений, щелкните отчет правой кнопкой мыши и выберите команду **Удалить отчет**.

Можно удалить несколько отчетов одновременно:

1. Выбирайте отчеты в списке, удерживая нажатой клавишу `Shift` или `Ctrl`.
2. Щелкните выбранные отчеты правой кнопкой мыши и выберите команду **Удалить отчеты**.

14

Сервер DeviceLock Content Security Server

В этой главе:

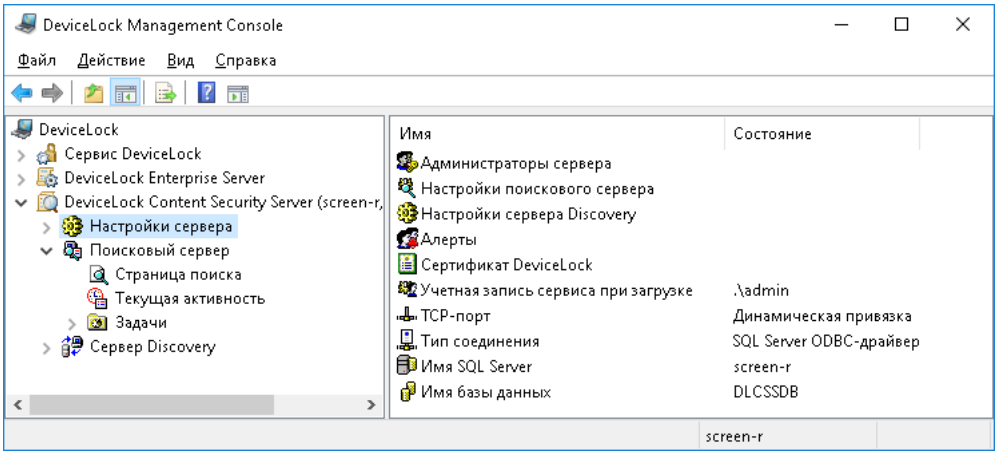
Администрирование сервера DeviceLock Content Security Server

Использование поискового сервера

Типы файлов, индексируемых для поиска

Администрирование сервера DeviceLock Content Security Server

Для настройки и использования сервера DeviceLock Content Security Server служит узел **DeviceLock Content Security Server** в консоли DeviceLock Management Console.



Щелкните правой кнопкой мыши узел **DeviceLock Content Security Server**, чтобы отобразить следующие команды:

- **Подключиться** - Подключает консоль к компьютеру, на котором работает DeviceLock Content Security Server. Подробнее см. в разделе Подключение к компьютеру.

  При подключении к компьютеру, на котором установлена более ранняя версия сервера DeviceLock Content Security Server, появляется следующее сообщение: “Версии продукта на машинах клиента и сервера не совпадают.” В таком случае необходимо установить новую версию DeviceLock Content Security Server на этот компьютер. Инструкции по установке см. в разделе Установка DeviceLock Content Security Server.

- **Переподключиться** - Подключается к текущему компьютеру повторно.

- **Подключаться к последнему использованному серверу при запуске** - Установите флажок рядом с этой командой, чтобы при каждом запуске консоль автоматически подключалась к серверу, который использовался в предыдущем подключении.

- **Мастер создания сертификата** - Запускает программу для создания сертификатов DeviceLock. Подробнее см. в разделе Создание сертификата.
- **Мастер создания подписи** - Запускает программу для авторизации устройств во временном белом списке и подписывания файлов с настройками сервиса DeviceLock. Подробнее см. в разделе Мастер создания подписи.
- **О программе DeviceLock** - Показывает диалоговое окно с информацией о версии и установленных лицензиях на DeviceLock.

Раскройте узел **DeviceLock Content Security Server**, чтобы отобразить следующие подчиненные узлы:

- **Настройки сервера** - Предоставляет доступ ко всем параметрам конфигурации сервера DeviceLock Content Security Server. Подробнее см. в разделе Настройки сервера.
- **Поисковый сервер** - Предоставляет доступ к функциям поискового сервера. Подробнее см. в разделе Использование поискового сервера.
- **Сервер Discovery** - Предоставляет доступ к функциям сервера Discovery. Подробнее о сервере Discovery см. в документе "Руководство пользователя DeviceLock Discovery".

Настройки сервера

Данный узел служит для настройки общих параметров сервера:

- **Администраторы сервера** - Задать список и права доступа администраторов сервера. Подробнее см. в разделе Администраторы сервера.
- **Настройки поискового сервера** - Задать параметры полнотекстового поиска. Подробнее см. в разделе Настройки поискового сервера.
- **Настройки сервера Discovery** - Задать параметры сервера DeviceLock Discovery.
- **Алерты** - Задать параметры тревожных оповещений сервера DeviceLock Discovery.
- **Сертификат DeviceLock** - Установить или удалить сертификат DeviceLock.
- **Учетная запись сервиса при загрузке** - Настроить данные стартовой учетной записи для запуска службы сервера (имя и пароль учетной записи).
- **TCP-порт** - Задать TCP-порт сервера для подключения консоли DeviceLock Management Console.
- **Тип соединения** - Выбрать драйвер ODBC или системный источник данных для доступа к серверу базы данных DeviceLock Content Security Server.
- **Имя SQL Server** - Указать сервер базы данных DeviceLock Content Security Server. Этот параметр отображается, если выбран тип соединения с использованием драйвера ODBC.
- **Системный источник данных** - Указать источник для доступа к серверу базы данных DeviceLock Content Security Server. Этот параметр отображается, если выбран тип соединения с использованием системного источника данных.
- **Имя базы данных** - Задать имя базы данных DeviceLock Content Security Server.
- **Имя пользователя SQL** - Указать логин и пароль для доступа к базе данных DeviceLock Content Security Server. Этот параметр отображается, если выбран режим "Аутентификация SQL Server".

Контекстное меню этого узла содержит следующую команду:

- **Свойства** - Запускает мастер управления параметрами сервера.

Подробнее см. в разделе Управление общими параметрами сервера.

Администраторы сервера

Узел **Администраторы сервера** определяет список и права доступа администраторов сервера DeviceLock Content Security Server, а также сертификат DeviceLock для данного сервера.

Контекстное меню этого узла содержит следующую команду:

- **Свойства** - Открывает диалоговое окно, в котором можно настроить список администраторов сервера и установить или удалить сертификат DeviceLock.

См. также:

Настройка доступа к DeviceLock Content Security Server

Установка или удаление сертификата DeviceLock

Администраторы сервера и сертификат

Настройки поискового сервера

Этот узел используется для настройки поискового сервера. Можно настроить следующие параметры:

- **DeviceLock Enterprise Server(ы)** - Указать серверы DeviceLock Enterprise Server, данные с которых будут индексироваться для полнотекстового поиска.
- **Директория индекса** - Задать место расположения полнотекстового индекса.
- **Интервал индексирования** - Задать промежуток времени в минутах между моментом завершения одного процесса индексирования и моментом начала следующего процесса индексирования.
- **Интервал слияния** - Задать промежуток времени в минутах, через который будут проходить операции слияния временных индексов в главный полнотекстовый индекс.
- **Извлекать текст из бинарных файлов** - Включить или отключить индексирование текстовых данных из не-текстовых (двоичных) файлов.
- **Извлекать текст из изображений (OCR)** - Включить или отключить оптическое распознавание (OCR) и индексирование текстовых данных на изображениях. Можно выбрать до 8 языков для распознавания.

  Примечание: Выбор нескольких азиатских языков (отмеченных звездочкой (*) на пользовательском интерфейсе), а также одновременный выбор азиатских и не азиатских языков может привести к значительному снижению производительности модуля OCR.

- **Лицензии поискового сервера** - Установить необходимое количество лицензий для поискового сервера.
- **Настройки уведомления** - Указать почтовый сервер (SMTP) для отправки отчетов поискового сервера.

Подробнее см. в разделе Управление параметрами поискового сервера.

Управление общими параметрами сервера

Имеется три группы параметров конфигурации сервера DeviceLock Content Security Server:

- **Общие параметры** - Влияют на работу сервера DeviceLock Content Security Server в целом. Инструкции по управлению этими параметрами приводятся далее в этом разделе.
- **Параметры поискового сервера** - Влияют на работу поискового сервера. Инструкции по управлению этими параметрами см. в разделе Управление параметрами поискового сервера.
- **Параметры сервера Discovery** - Влияют на работу сервера Discovery. Подробнее об этих параметрах см. в разделе "Параметры сервера Discovery" документа "Руководство пользователя DeviceLock Discovery".

Настроить общие параметры можно в процессе первоначальной установки сервера DeviceLock Content Security Server. После того как сервер установлен и работает, можно использовать консоль DeviceLock Management Console для просмотра и изменения этих параметров.

Примечание:

- Чтобы управлять и пользоваться сервером DeviceLock Content Security Server, необходимо быть администратором сервера с достаточными правами доступа.
- Консоль DeviceLock Management Console необходимо подключить к компьютеру, на котором работает сервер DeviceLock Content Security Server. Для этого в дереве консоли щелкните правой кнопкой мыши **DeviceLock Content Security Server** и выберите команду **Подключиться**. Подробнее см. в разделе Подключение к компьютеру.

С помощью DeviceLock Management Console можно выполнить следующие задачи настройки сервера:

- Указать, какие пользователи имеют доступ к серверу DeviceLock Content Security Server.
- Изменить данные стартовой учетной записи для запуска службы DeviceLock Content Security Server (имя и пароль учетной записи).
- Установить или удалить сертификат DeviceLock для авторизации соединений между сервером DeviceLock Content Security Server и сервером DeviceLock Enterprise Server.
- Изменить TCP-порт сервера DeviceLock Content Security Server для подключения консоли DeviceLock Management Console.
- Проверить или изменить параметры соединения с базой данных сервера DeviceLock Content Security Server.

Эти задачи можно выполнять все сразу или по отдельности. В первом случае используется мастер настройки, который запускается автоматически при установке или обновлении сервера DeviceLock Content Security Server.

Чтобы выполнить настройку сервера с помощью мастера настройки

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** щелкните правой кнопкой мыши **Настройки сервера**, а затем выберите команду **Свойства**.

   Появится первая страница мастера настройки.
3. Пройдите через все страницы мастера. После завершения работы с каждой страницей нажимайте кнопку **Далее**, чтобы перейти на следующую страницу. Чтобы вернуться на предыдущую страницу, нажмите кнопку **Назад**. На последней странице нажмите кнопку **Готово** для завершения работы мастера.

   Описание страниц мастера см. в разделе Настройка и завершение установки инструкции Установка DeviceLock Content Security Server.

С помощью консоли DeviceLock Management Console можно выполнять следующие задачи по настройке отдельных параметров сервера:

- Настройка доступа к DeviceLock Content Security Server
- Настройка стартовой учетной записи службы сервера
- Установка или удаление сертификата DeviceLock
- Настройка параметра TCP-порт
- Настройка подключения к базе данных

Настройка доступа к DeviceLock Content Security Server

Предусмотрена возможность указать, кому именно разрешено работать с сервером DeviceLock Content Security Server. Это позволяет защитить сервер от несанкционированного доступа и внешних атак.

Чтобы указать, какие пользователи имеют доступ к серверу

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** выполните одно из следующих действий:
   - Выберите **Настройки сервера**. На панели сведений дважды щелкните **Администраторы сервера** или щелкните правой кнопкой мыши **Администраторы сервера** и затем выберите команду **Свойства**.

     - или -
   - Раскройте узел **Настройки сервера**. В узле **Настройки сервера** щелкните правой кнопкой мыши **Администраторы сервера**, а затем выберите команду **Свойства**.
3. В появившемся диалоговом окне **DeviceLock Content Security Server** выполните следующие действия:

   Чтобы включить защиту по умолчанию

   - Установите флажок **Включить безопасность по умолчанию**.

   Если включена защита по умолчанию, члены локальной группы Администраторы получат полный доступ к DeviceLock Content Security Server.

   Чтобы предоставить доступ к серверу отдельным пользователям

   a) Снимите флажок **Включить безопасность по умолчанию**.

   b) Под областью **Пользователи** нажмите кнопку **Добавить**, чтобы добавить пользователей, которым необходимо предоставить доступ к серверу DeviceLock Content Security Server.

   c) В появившемся диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, а затем нажмите кнопку **OK**.

   Выбранные пользователи/группы становятся администраторами сервера и отображаются в области **Пользователи** диалогового окна **DeviceLock Content Security Server**. Администраторы сервера имеют право выполнять задачи, связанные с настройкой и использованием сервера DeviceLock Content Security Server, и по умолчанию они имеют полный доступ к серверу.

Чтобы изменить уровень доступа к серверу для какого-либо администратора, выберите соответствующего пользователя или группу в области **Пользователи**, а затем в списке прав доступа выберите один из следующих вариантов:

- **Полный доступ** - Позволяет устанавливать и удалять сервер DeviceLock Content Security Server, подключаться к нему с помощью консоли DeviceLock Management Console и выполнять любые действия на сервере, в том числе: просматривать и изменять настройки сервера; создавать и запускать поисковые запросы и задачи; просматривать и изменять настройки обнаружения контента; создавать и запускать задачи и отчеты обнаружения контента.
- **Изменение** - То же, что и полный доступ к серверу, за исключением права вносить изменения в список администраторов сервера, а также права изменять уровень доступа к серверу для пользователей и групп, уже имеющихся в этом списке.
- **Только чтение** - Позволяет подключаться к серверу DeviceLock Content Security Server с помощью консоли DeviceLock Management Console, просматривать настройки сервера, выполнять поисковые запросы, просматривать и запускать уже имеющиеся поисковые задачи, просматривать настройки обнаружения контента, а также просматривать отчеты по результатам сканирования и обнаружения и вручную создавать новые отчеты на основе существующих отчетов и данных, подготовленных задачами сканирования и обнаружения контента. Не позволяет запускать такие задачи, вносить какие-либо изменения на сервере, или создавать новый индекс для поискового сервера.

Для пользователей и групп с уровнем доступа **Изменение** или **Только чтение** можно выбрать опцию **Доступ к теневым копиям**, чтобы обеспечить доступ к теневым копиям и записям активности пользователей. Пользователи и группы, для которых выбрана эта опция, могут выполнять поиск по содержимому теневых копий и записей активности пользователей, а также открывать, просматривать и сохранять теневые копии и записи активности пользователей, обнаруженные в результате поиска.

Администраторы сервера DeviceLock Content Security Server, у которых нет доступа к теневым копиям, не могут открывать, просматривать и сохранять теневые копии и записи активности пользователей. На результатах поиска нет ссылок **Открыть**, **Сохранить** и **Просмотр**, а вместо текстовых фрагментов теневых копий и записей активности пользователей отображаются звездочки. Логины и пароли в параметрах документа для записей активности пользователей также заменяются звездочками.

Внимание: Настоятельно рекомендуется, чтобы администраторам DeviceLock Content Security Server были предоставлены права локального администратора.

Чтобы отозвать права администратора сервера у какого-либо пользователя или группы, выберите этого пользователя или группу в области **Пользователи**, а затем нажмите кнопку **Удалить**.

Чтобы выбрать одновременно несколько пользователей или групп, используйте клавиши SHIFT или CTRL.

4. Нажмите кнопку **OK**.

Настройка стартовой учетной записи службы сервера

Спустя какое-то время может понадобиться изменить стартовую учетную запись службы сервера DeviceLock Content Security Server, выбранную в процессе установки. Также может потребоваться изменить пароль этой учетной записи.

Чтобы изменить имя или пароль стартовой учетной записи службы сервера

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** выберите **Настройки сервера**.
3. На панели сведений дважды щелкните **Учетная запись сервиса при загрузке** или щелкните правой кнопкой мыши **Учетная запись сервиса при загрузке** и затем выберите команду **Свойства**.
4. В появившемся диалоговом окне **DeviceLock Content Security Server** выполните следующие действия:

   Чтобы изменить стартовую учетную запись службы сервера

   a) В области **Входить в систему как** нажмите кнопку **Обзор**.

   b) В появившемся диалоговом окне **Выбор: "Пользователь"** в поле **Введите имена выбираемых объектов** введите имя пользователя, а затем нажмите кнопку **OK**.

   Выбранный пользователь отображается в поле **Данная учетная запись** диалогового окна **DeviceLock Content Security Server**.

   Настоятельно рекомендуется использовать учетную запись, обладающую правами администратора на всех компьютерах, где установлен сервер DeviceLock Enterprise Server. В домене Active Directory рекомендуется использовать учетную запись, являющуюся членом группы “Администраторы домена”. В противном случае будет необходимо использовать авторизацию по сертификату DeviceLock.

   Чтобы изменить пароль учетной записи службы сервера

   a) В области **Входить в систему как** введите новый пароль в поле **Пароль**.

   b) Повторно введите новый пароль в поле **Подтверждение пароля**.

   Чтобы назначить учетную запись СИСТЕМА для службы сервера

   - В области **Входить в систему как** выберите опцию **Локальная учетная запись системы**.

   Внимание: Поскольку учетная запись СИСТЕМА не может использоваться для аутентификации при подключении к серверу DeviceLock Enterprise Server на удаленных компьютерах, в этом случае должна использоваться аутентификация по сертификату DeviceLock.

5. Нажмите кнопку **OK**.

Установка или удаление сертификата DeviceLock

Если стартовая учетная запись службы DeviceLock Content Security Server не может пройти аутентификацию при получении доступа к удаленному серверу DeviceLock Enterprise Server, необходимо использовать аутентификацию по сертификату DeviceLock. Для этого установите секретный ключ одного и того же сертификата на сервере DeviceLock Content Security Server и на сервере DeviceLock Enterprise Server. Подробнее о сертификатах DeviceLock см. в разделе Сертификаты DeviceLock.

Чтобы установить или удалить сертификат DeviceLock на сервере DeviceLock Content Security Server

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** выберите **Настройки сервера**.
3. На панели сведений дважды щелкните **Сертификат DeviceLock** или щелкните правой кнопкой мыши **Сертификат DeviceLock** и затем выберите команду **Свойства**.
4. В появившемся диалоговом окне **DeviceLock Content Security Server** выполните следующие действия:

   Чтобы установить секретный ключ сертификата DeviceLock

   a) Нажмите кнопку ··· рядом с полем **Имя сертификата**, чтобы открыть диалоговое окно **Выберите файл сертификата DeviceLock**.

   b) В диалоговом окне **Выберите файл сертификата DeviceLock** выберите соответствующий файл сертификата, и нажмите кнопку **Открыть**.

   Имя сертификата появится в поле **Имя сертификата** диалогового окна **DeviceLock Content Security Server**.

   Чтобы удалить секретный ключ сертификата DeviceLock

   - Нажмите кнопку **Удалить** рядом с полем **Имя сертификата**.
5. Нажмите кнопку **OK**.

Настройка параметра TCP-порт

Спустя какое-то время может понадобиться изменить TCP-порт для подключения консоли DeviceLock Management Console к серверу DeviceLock Content Security Server.

Чтобы изменить TCP-порт для подключения консоли

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** выберите **Настройки сервера**.
3. На панели сведений дважды щелкните **TCP-порт** или щелкните правой кнопкой мыши **TCP-порт** и затем выберите команду **Свойства**.
4. В области **Настройки подключения** появившегося диалогового окна **DeviceLock Content Security Server** выполните одно из следующих действий:

   - Щелкните **Динамическая привязка портов**, чтобы использовать динамический выбор порта.

     - или -

   - Щелкните **Фиксированный TCP-порт**, чтобы использовать заданный порт. Затем введите требуемый номер порта в поле **Фиксированный TCP-порт**.

     По умолчанию DeviceLock Content Security Server использует порт 9134.
5. Нажмите кнопку **OK**.

Настройка подключения к базе данных

Подключение к базе данных необходимо для работы поискового сервера и сервера Discovery. При отсутствии подключения к базе данных невозможен поиск с использованием контентно-зависимых групп, сохранение и автоматизация поисковых запросов, а также сканирование и обнаружение контента при помощи сервера Discovery. Используя консоль, можно просмотреть или изменить параметры подключения к базе данных.

Чтобы просмотреть или изменить параметры подключения к базе данных

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** выберите **Настройки сервера**.
3. На панели сведений дважды щелкните любой из следующих параметров: **Тип соединения**, **Имя SQL Server**, **Имя базы данных** или **Имя пользователя SQL**. Можно также щелкнуть параметр правой кнопкой мыши и затем выбрать команду **Свойства**.
4. В появившемся диалоговом окне можно просмотреть или изменить следующие параметры:
   - **Имя базы данных** - Имя базы данных сервера DeviceLock Content Security Server.
   - **Тип соединения** - Определяет, использовать ли драйвер ODBC или системный источник данных для соединения с сервером базы данных DeviceLock Content Security Server.

     Дальнейшие параметры зависят от выбранного типа соединения.
   - **Имя SQL Server** - Имя сервера базы данных (если используется драйвер ODBC).

     Пустое имя означает, что сервер базы данных находится на компьютере, на котором работает DeviceLock Content Security Server.
   - **Аутентификация Windows** / **Аутентификация SQL Server** - Режим аутентификации на SQL-сервере (для драйвера ODBC Microsoft SQL Server).
   - **Имя источника данных** - Имя системного источника данных (если используется системный источник данных).
   - **Имя пользователя**, **Пароль** - Логин и пароль для доступа к базе данных (при использовании режима “Аутентификация SQL Server”).
5. Нажмите кнопку **Далее** и дождитесь завершения операции. Затем нажмите кнопку **Готово**.

Подробнее о параметрах подключения к базе данных см. в разделе Настройка базы данных инструкции Установка DeviceLock Content Security Server.

Управление параметрами поискового сервера

Параметры поискового сервера относятся к полнотекстовому поиску и применяются только к поисковому серверу - одному из компонентов сервера DeviceLock Content Security Server.

В процессе установки сервера DeviceLock Content Security Server можно только установить лицензии на поисковый сервер. Для настройки параметров поискового сервера используется консоль DeviceLock Management Console.

Ниже приведены пошаговые инструкции, объясняющие, как с помощью консоли DeviceLock Management Console управлять параметрами поискового сервера:

- Лицензии поискового сервера
- Серверы DeviceLock Enterprise Server для индексирования
- Местоположение индекса поискового сервера
- Извлечения текстовых данных из двоичных файлов
- Расписание индексирования
- Расписание операций слияния индексов
- Построение нового индекса по запросу
- Обновление существующего индекса по запросу
- Проверка текущего состояния процесса индексирования
- Почтовый сервер для отчетов поискового сервера

Лицензии поискового сервера

Для использования сервера DeviceLock Content Security Server необходимо приобрести специальную лицензию на поисковый сервер. Одну и ту же лицензию можно использовать на всех компьютерах, где устанавливается сервер DeviceLock Content Security Server.

Лицензирование поискового сервера основано на количестве записей в журналах, которые будут индексироваться для полнотекстового поиска. Каждая лицензия позволяет индексировать 1 000 записей в журнале теневого копирования (включая теневые копии документов), 1 000 записей в журнале активности пользователей (включая записи ввода с клавиатуры) и по 5 000 записей в каждом из прочих журналов (журнал аудита, журнал удаленных данных теневого копирования, журнал сервера, журнал мониторинга и журнал политик).

Требуемое количество лицензий поискового сервера зависит от количества записей в журналах сервера DeviceLock Enterprise Server. Максимально возможное количество индексируемых записей вычисляется исходя из общего числа установленных лицензий. При необходимости можно приобрести и установить дополнительные лицензии. Пробный период для сервера DeviceLock Content Security Server составляет 30 дней. В течение этого периода сервер может индексировать 2 000 записей в журнале теневого копирования, 2 000 записей в журнале активности пользователей и по 10 000 записей в каждом из прочих журналов.

Чтобы установить лицензии для поискового сервера

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**, а затем раскройте узел **Настройки сервера**.
2. В узле **Настройки сервера** выберите **Настройки поискового сервера**.
3. На панели сведений дважды щелкните **Лицензии поискового сервера** или щелкните правой кнопкой мыши **Лицензии поискового сервера** и затем выберите команду **Свойства**.

   Появится диалоговое окно “DeviceLock Content Security Server”.

4. В диалоговом окне **DeviceLock Content Security Server** нажмите кнопку **Загрузить лицензии**.
5. В появившемся диалоговом окне выберите файл лицензии и нажмите кнопку **Открыть**.

   После загрузки файла лицензий можно просмотреть сводную информацию: в строке "Всего лицензий" отображается общее количество приобретенных лицензий, а строка "Использовано лицензий" содержит количество лицензий, использованных на данный момент для индексации данных из журналов DeviceLock Enterprise Server.

   Можно установить столько лицензий, сколько необходимо для удовлетворения нужд организации. Для этого загрузите файлы лицензий один за другим.
6. Нажмите кнопку **OK**.

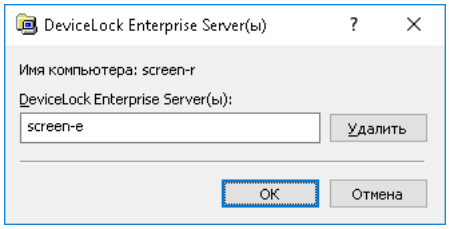
Серверы DeviceLock Enterprise Server для индексирования

Для создания поискового индекса необходимо указать хотя бы один сервер DeviceLock Enterprise Server. Индексирование начинается автоматически, как только указан сервер DeviceLock Enterprise Server.

Чтобы задать сервер или серверы DeviceLock Enterprise Server

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**, а затем раскройте узел **Настройки сервера**.
2. В узле **Настройки сервера** выберите **Настройки поискового сервера**.
3. На панели сведений дважды щелкните **DeviceLock Enterprise Server(ы)** или щелкните правой кнопкой мыши **DeviceLock Enterprise Server(ы)** и затем выберите команду **Свойства**.

   Появится диалоговое окно "DeviceLock Enterprise Server(ы)".



4. В диалоговом окне **DeviceLock Enterprise Server(ы)** введите IP-адрес или имя компьютера, на котором работает DeviceLock Enterprise Server.

   Если имен или IP-адресов несколько, разделяйте их точкой с запятой (;).

   Примечание: Убедитесь, что сервер DeviceLock Enterprise Server установлен надлежащим образом и доступен для сервера DeviceLock Content Security Server, в противном случае данные с этого сервера не будут индексироваться поисковым сервером.

   Чтобы удалить имена компьютеров или IP-адреса, нажмите кнопку **Удалить**.
5. Нажмите кнопку **OK**.

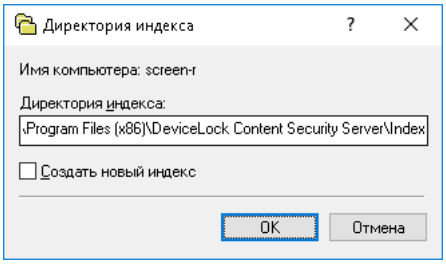
Местоположение индекса поискового сервера

Имеется возможность указать папку для расположения индекса. Если папка не указана, то индекс располагается в папке по умолчанию `%ProgramFiles%\DeviceLock Content Security Server\Index`. Поисковый сервер начинает индексирование автоматически каждый раз, когда указывается новое место расположения индекса.

Чтобы указать место расположения индекса

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**, а затем раскройте узел **Настройки сервера**.
2. В узле **Настройки сервера** выберите **Настройки поискового сервера**.
3. На панели сведений дважды щелкните **Директория индекса** или щелкните правой кнопкой мыши **Директория индекса** и затем выберите команду **Свойства**.

   Появится диалоговое окно "Директория индекса".



4. В поле **Директория индекса** введите путь к папке, в которой нужно разместить индекс.

   Если требуется создать новый индекс немедленно, установите флажок **Создать новый индекс**.

   Если в указанном месте уже находится индекс и вы создаете новый индекс, появится окно с сообщением: "Вы действительно хотите создать новый индекс и переписать существующий (Да - переписать, Нет - дополнить)?" В этом окне нажмите кнопку "Да", чтобы полностью перестроить полнотекстовый индекс немедленно. Нажмите кнопку "Нет", чтобы обновить существующий полнотекстовый индекс немедленно.
5. Нажмите кнопку **OK**.

Извлечения текстовых данных из двоичных файлов

Имеется возможность разрешить или запретить извлечение и индексирование текста из двоичных, не-текстовых файлов.

Чтобы разрешить или запретить извлечение текста из двоичных файлов

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**, а затем раскройте узел **Настройки сервера**.
2. В узле **Настройки сервера** выберите **Настройки поискового сервера**.
3. На панели сведений дважды щелкните **Извлекать текст из бинарных файлов** или щелкните правой кнопкой мыши **Извлекать текст из бинарных файлов** и затем выберите команду **Включить** или **Выключить**.

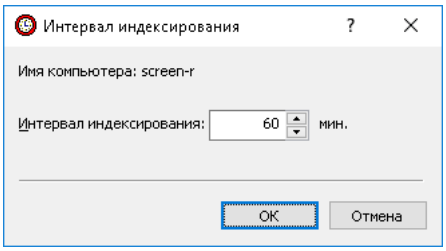
Расписание индексирования

Поисковый сервер обеспечивает создание и обновление поискового индекса по расписанию. Расписание индексирования основано на интервале индексирования, который представляет собой интервал времени между окончанием текущего сеанса индексирования и началом следующего сеанса индексирования. По умолчанию этот интервал составляет 60 минут.

Чтобы настроить расписание индексирования

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**, а затем раскройте узел **Настройки сервера**.
2. В узле **Настройки сервера** выберите **Настройки поискового сервера**.
3. На панели сведений дважды щелкните **Интервал индексирования** или щелкните правой кнопкой мыши **Интервал индексирования** и затем выберите команду **Свойства**.

   Появится диалоговое окно "Интервал индексирования".



4. В поле **Интервал индексирования** введите или выберите требуемое число минут для интервала индексирования.
5. Нажмите кнопку **OK**.

Расписание операций слияния индексов

Выполняя слияние индексов по расписанию, поисковый сервер объединяет временные индексы в рабочий индекс для обслуживания поисковых запросов. Это расписание основано на интервале слияния, определяющем, как часто рабочий индекс пополняется новыми данными из временных индексов. Можно задать интервал слияния от 1 до 100 000 минут. Значение по умолчанию составляет 10 минут.

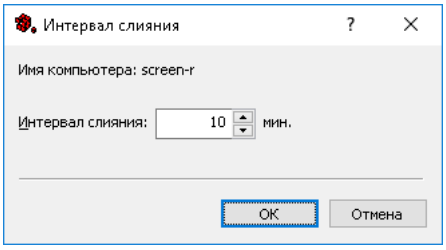
При выборе значения интервала слияния учитывайте следующее:

- Чем меньше интервал слияния, тем быстрее завершается слияние индексов.
- Сервер не может выполнять поисковые запросы, пока слияние индексов не завершено.

Чтобы настроить расписание операций слияния индексов

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**, а затем раскройте узел **Настройки сервера**.
2. В узле **Настройки сервера** выберите **Настройки поискового сервера**.
3. На панели сведений дважды щелкните **Интервал слияния** или щелкните правой кнопкой мыши **Интервал слияния** и затем выберите команду **Свойства**.

Появится диалоговое окно “Интервал слияния”.



4. В поле **Интервал слияния** введите или выберите требуемое число минут для интервала слияния.
5. Нажмите кнопку **OK**.

Построение нового индекса по запросу

Можно полностью перестроить полнотекстовый индекс немедленно.

Чтобы перестроить полнотекстовый индекс немедленно

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** щелкните правой кнопкой мыши **Поисковый сервер**, а затем выберите команду **Создать новый индекс**.

   Если индекс уже существует и вы создаете новый индекс, появится окно со следующим сообщением: “Вы действительно хотите создать новый индекс и переписать существующий (Да - переписать, Нет - дополнить)?” В этом окне нажмите кнопку “Да”, чтобы полностью перестроить полнотекстовый индекс немедленно. Нажмите кнопку “Нет”, чтобы обновить существующий полнотекстовый индекс немедленно.

Обновление существующего индекса по запросу

При необходимости срочно проиндексировать новые данные, появившиеся на сервере DeviceLock Enterprise Server, можно немедленно обновить существующий индекс с учетом этих новых данных, не дожидаясь запланированного обновления индекса по расписанию.

Чтобы обновить существующий индекс немедленно

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** щелкните правой кнопкой мыши **Поисковый сервер**, а затем выберите команду **Проиндексировать**.

   При обновлении индекса поисковый сервер не перестраивает индекс полностью. Он индексирует только новые данные сервера DeviceLock Enterprise Server для добавления новых записей в существующий индекс.

Проверка текущего состояния процесса индексирования

Узел **Текущая активность** служит для проверки состояния процесса индексирования.

Операции полнотекстового индексирования могут занимать много времени и ресурсов. Поисковый сервер позволяет наблюдать за ходом выполнения операций индексирования, выполняющихся в данный момент.

Процесс индексирования выполняется в два этапа. На первом этапе поисковый сервер извлекает ключевые слова из теневых копий и записей в журналах и сохраняет их во временные индексы для каждого указанного сервера DeviceLock Enterprise Server. Для каждого временного индекса поисковый сервер обрабатывает 1000 записей из каждого журнала.

На втором этапе, когда число временных индексов становится равным 50 или проходит 10 минут, инициируется процесс объединения всех временных индексов в один главный полнотекстовый индекс, который используется для поисковых запросов. Процесс объединения временных индексов в главный полнотекстовый индекс называется слиянием.

Если в дереве консоли выбрать узел **Текущая активность**, на панели сведений отобразятся индикаторы состояния и хода выполнения операций индексирования и слияния.

Индикаторы состояния и хода выполнения операции индексирования

Процесс индексирования для каждого заданного сервера DeviceLock Enterprise Server можно контролировать по индикаторам состояния и хода выполнения операции. Индикатор состояния показывает текущее состояние операции индексирования:

Состояние	Описание
Бездействие	Индексирование не выполняется.
Ожидание	Ожидается начало индексирования.
Индексирование <имя журнала>	Выполняется индексирование указанного журнала.

Индикатор хода выполнения показывает процент завершения процесса индексирования.

Индикаторы состояния и хода выполнения операции слияния индексов

Процесс слияния индексов можно контролировать, наблюдая за индикаторами его состояния и хода выполнения. Индикатор состояния показывает текущее состояние операции слияния:

Состояние	Описание
Бездействие	Слияние индексов не выполняется.
Слияние	Выполняется слияние индексов.
Дефрагментация	Выполняется сжатие и оптимизация индекса путем удаления устаревших данных и консолидации с целью повышения эффективности поиска.

Индикатор хода выполнения показывает процент завершения процесса слияния.

Чтобы проверить состояние индексирования и слияния

1. В дереве консоли раскройте узлы **DeviceLock Content Security Server** > **Поисковый сервер**.
2. В узле **Поисковый сервер** выберите **Текущая активность**.

Если в дереве консоли выбрана **Текущая активность**, на панели сведений отображаются индикаторы состояния и хода выполнения операций индексирования и слияния индексов. Поскольку индикаторы не обновляются автоматически, их необходимо обновлять вручную:

- Щелкните правой кнопкой мыши **Текущая активность** и выберите команду **Обновить**.

  - или -

- Выберите **Текущая активность** и щелкните на панели инструментов.

  - или -

- На панели сведений щелкните правой кнопкой мыши любое имя сервера DeviceLock Enterprise Server или **Объединить индекс**, а затем выберите команду **Обновить**.

  - или -

- На панели сведений выберите любое имя сервера DeviceLock Enterprise Server или **Объединить индекс**, а затем щелкните на панели инструментов.

Почтовый сервер для отчетов поискового сервера

Поисковый сервер использует почтовый сервер SMTP для доставки отчетов с результатами поиска. Почтовый сервер можно задать с помощью команды **Настройки уведомления** в контекстном меню узла **Поисковый сервер** или с помощью параметра **Настройки уведомления** в узле **Настройки поискового сервера**.

Чтобы задать почтовый сервер для доставки отчетов поискового сервера

1. В дереве консоли раскройте узел **DeviceLock Content Security Server**.
2. В узле **DeviceLock Content Security Server** щелкните правой кнопкой мыши **Поисковый сервер**, а затем выберите команду **Настройки уведомления**.

   Можно также раскрыть узел **Настройки сервера**, выбрать **Настройки поискового сервера** в дереве консоли, а затем дважды щелкнуть **Настройки уведомления** на панели сведений.
3. В открывшемся диалоговом окне установите флажок **Отправлять уведомления по e-mail для отчетов** и укажите следующие параметры почтового сервера:
   - **SMTP-сервер** - Имя или IP-адрес SMTP-сервера для отправки отчетов.
   - **Порт** - Порт для подключения к SMTP-серверу. По умолчанию установлен порт 25. Снимите флажок **По умолчанию**, если требуется ввести другой номер порта.

     Примечание: DeviceLock поддерживает как незащищенные, так и защищенные (SSL) подключения к SMTP-серверу. Тип подключения устанавливается автоматически, в зависимости от того, включен ли SSL на SMTP-сервере.
   - **Сервер требует аутентификацию** - Установите этот флажок, если для подключения к указанному SMTP-серверу требуется аутентификация. Снимите этот флажок, если аутентификация не требуется.

     Если флажок **Сервер требует аутентификацию** установлен, в поле **Имя пользователя** и **Пароль** необходимо указать имя и пароль учетной записи электронной почты, у которой есть разрешение на подключение к SMTP-серверу.
   - **Адрес отправителя** - Укажите адрес для отображения в поле **От** сообщений электронной почты с отчетами поискового сервера.
4. Для проверки заданных параметров почтового сервера нажмите кнопку **Тест**.
5. В диалоговом окне, которое открывается по нажатию кнопки **Тест**, укажите электронный адрес получателя и нажмите кнопку **OK** для отправки тестового письма.

   Если параметры почтового сервера указаны правильно, письмо будет доставлено получателю. В противном случае консоль отобразит сообщение с описанием проблемы.
6. По завершении нажмите кнопку **OK**.

Использование поискового сервера

Входящий в состав сервера DeviceLock Content Security Server поисковый сервер обеспечивает поиск данных, хранящихся в журналах сервера DeviceLock Enterprise Server. Возможен поиск текстовых фрагментов (полнотекстовый поиск), а также поиск объектов данных по различным признакам, таким как типы файлов, ключевые слова или свойства документов (см. Управление контентно-зависимыми группами поиска). Все эти возможности поискового сервера упрощают и делают более эффективным анализ больших объемов данных, накапливающихся в журналах сервера DeviceLock Enterprise Server.

Контекстное меню узла **Поисковый сервер** содержит следующие команды:

- **Создать новый индекс** - Немедленно начинает перестраивать весь поисковый индекс. Подробнее см. в разделе Построение нового индекса по запросу.
- **Проиндексировать** - Немедленно начинает обновлять существующий поисковый индекс. Подробнее см. в разделе Обновление существующего индекса по запросу.
- **Настройки уведомления** - Задает почтовый сервер SMTP для доставки отчетов. Подробнее см. в разделе Почтовый сервер для отчетов поискового сервера.

Использование поискового сервера предполагает следующие действия:

- Выполнение поиска
- Работа с результатами поиска
- Автоматизация поиска

Выполнение поиска

Поисковый сервер позволяет найти все записи во всех журналах сервера DeviceLock Enterprise Server, где встречается определенное слово или текстовый фрагмент. Поскольку поисковые запросы обычно возвращают большое количество результатов, предусмотрен ряд параметров для точной настройки и оптимизации поиска. Эти параметры позволяют указать, какие именно результаты должен возвращать поиск.

С помощью параметров поиска можно:

- Фильтровать результаты поиска по дате, журналу, отправителю, получателю, типу файла, источнику и т.п. Например, фильтр позволяет ограничить результаты поиска определенными журналами и заданным диапазоном дат.
- Задать количество результатов поиска на страницу.

Описание параметров поиска, а также инструкцию по настройке и выполнению поиска, см. в разделе Действия по выполнению поиска.

После завершения поиска сервер возвращает страницу результатов, состоящую из нескольких областей:

- Область запроса - Отображает заданные критерии поиска.
- Строка статистики - Показывает количество результатов поиска, отображённых на текущей странице результатов.
- Область результатов поиска - Отображает нумерованный список найденных результатов, соответствующих заданным критериям поиска.
- Навигатор результатов - Показывает количество страниц с результатами поиска и позволяет переходить с одной страницы на другую.

Подробнее о странице результатов поиска см. в разделе Работа с результатами поиска.

При использовании полнотекстового поиска важно учитывать следующее:

- Возможен поиск по отдельным полям, которые представлены в разделах **Параметры журнала** и **Параметры документа** результата поиска. Для этого используется следующий синтаксис: `<Имя поля>::<Значение>`. Пример: `Имя файла::Prices.docx`.

  Для поиска можно использовать несколько пар имя-значение поля, взяв каждую такую пару в скобки. Например, результатом поиска `(Имя файла::secret) (Тип файла::Excel)` будут файлы Excel, содержащие слово `secret` в имени файла.

  Внимание: Имена полей следует указывать с учетом регистра. Строчные и прописные буквы в имени поля различаются.

- При поиске в журнале активности пользователей выполняется также поиск в записях ввода с клавиатуры. Возможен поиск фрагментов текста и паролей, которые вводил пользователь. Поиск паролей выполняется по значению поля `Пароли` записи активности пользователей: `Пароли::<Значение>`. Например, для поиска записей, содержащих какие-либо пароли, используйте следующий синтаксис: `Пароли::?*` (звездочка без вопросительного знака соответствовала бы любому паролю или отсутствию пароля).
- В строке поискового запроса можно указывать логические операторы, такие как `AND` (И) и `OR` (ИЛИ). Пробел между словами трактуется как `AND`. Точка с запятой (;) трактуется как `OR`. Логические операторы необходимо печатать большими буквами. Подробнее см. в разделе Обзор логических операторов.
- При выполнении поиска не учитывается регистр букв в строке поискового запроса, за исключением поиска по значению поля. Имена полей чувствительны к регистру.
- Стемминг (морфологический поиск) включен по умолчанию. Стемминг обеспечивает поиск вариантов заданного слова по его грамматической основе. Поддерживается для английского, испанского, итальянского, немецкого, португальского, русского и французского языков. Например, запрос `applied` обнаружит также слова `applying`, `applies` и `apply`.
- В строке поискового запроса можно использовать знаки подстановки звездочка (*) и вопросительный знак (?). Звездочка обозначает произвольный набор символов или их отсутствие. Вопросительный знак обозначает произвольный одиночный символ. Знаки подстановки можно использовать в любом месте строки и в любом количестве.
- Для поиска определенной фразы необходимо заключить ее в двойные кавычки в строке поискового запроса. Для поиска нескольких слов необходимо разделить их пробелами.

В следующей таблице приводятся примеры и результаты различных вариантов поиска.

Вариант поиска	Пример	Результаты поиска
Отдельное слово	price	Все результаты, содержащие слово `price`. Будут найдены также различные грамматические формы слова, такие как `prices`, `priced` и т.п.
Фраза	confidential information	Все результаты, содержащие оба слова `confidential` и `information` в любом сочетании.
	“confidential information”	Все результаты, содержащие точное совпадение фразы `confidential information`.

Вариант поиска	Пример	Результаты поиска
Поиск с использованием знаков подстановки	te?t	Все результаты, содержащие слова `test`, `text` и т.п.
	mone*	Все результаты, содержащие слова `money`, `monetary` и т.п.
	*air	Все результаты, содержащие слова `air`, `fair`, `impair`, `affair` и т.п.
	"* assets"	Все результаты, содержащие фразы, которые заканчиваются словом `assets`, например: `monetary assets`, `liquid assets`, `fixed assets`, `current assets`.
Булевский поиск См. также Обзор логических операторов	price AND quality	Все результаты, содержащие оба слова `price` и `quality`.
	price quality	
	price OR quality	Все результаты, содержащие слово `price` или `quality`, или оба этих слова.
	price; quality	
Поиск по полям	(Действие::Message) (Получатель:: john.smith@domain.com) (Вложения::.doc) (Вложения::.pdf)	Все сообщения электронной почты с вложенными `.pdf` и `.doc` файлами, отправленные на адрес `john.smith@domain.com`.
	(Действие::Chat) (Имя файла::Mike)	Все мгновенные сообщения, отправленные для/от пользователя `Mike`.
	(Имя файла::secret) (Тип файла::Excel)	Файлы Excel, содержащие слово `secret` в имени файла и переданные по любому поддерживаемому каналу.
	(Тип файла::Acrobat) (Источник::File Sharing) (Размер файла::100~~200 MB)	Файлы PDF размером от `100` до `200` МБ, загруженные на сайты обмена файлами или скачанные с таких сайтов.

Поисковый сервер поддерживает также расширенный синтаксис поисковых запросов.

Символ	Значение	Описание
=	Любая цифра	Выражение `N===` будет соответствовать выражению `N123`, но не выражению `N1234` или `Nabc`.
-	Исключается	Поместите символ – (черточка) в начале любого слова или выражения, которое должно быть исключено из результата поиска. Пример: `-"monetary assets"`
%	Нечеткий поиск	Нечеткий поиск позволяет находить слова, даже если они написаны с ошибкой. Количество символов `%` определяет количество различий, игнорируемых при поиске слова. Позиция символов `%` определяет, сколько символов в начале слова должно точно соответствовать поисковому запросу. Нечеткий поиск может быть полезен при поиске в тексте, содержащем слова с опечатками. Например, поисковый запрос `inf%%ormation` возвратит все слова, начинающиеся с `inf` и написанные не более чем с двумя отличиями от слова `information`.

Символ	Значение	Описание
#	Фонетический поиск	Фонетический поиск возвращает слова, звучащие подобно заданному слову и начинающие с той же буквы. Такой поиск несколько медленнее других видов поиска. Поддерживается только для английского языка. Например, поисковый запрос `#smith` возвратит результаты `smithe` и `smythe`.
&	Поиск синонимов	Синонимический поиск возвращает слова-синонимы заданного слову. Поддерживается только для английского и русского языков. Например, поисковый запрос `fast&` возвратит также результат `quickly`.
~~	Числовой диапазон	Поиск в числовом диапазоне служит для поиска любых чисел в пределах указанного диапазона. Для задания такого запроса следует указать нижнюю и верхнюю границы диапазона, разделенные символами `~~`. Значения, указанные как нижняя и верхняя границы, также включаются в результаты поиска. Разделители, такие как десятичная точка и запятая, заменяются на пробелы, знак минуса игнорируется. Например, поисковый запрос `500~~1000` возвратит текст, содержащий числа в промежутке между `500` и `1000`.
:	Вес выражения	По умолчанию все слова в результатах поиска имеют одинаковый вес при подсчете. Данное условие поиска позволяет задать относительный вес для каждого выражения в поисковом запросе. Например, поисковый запрос `money:5 information:1` возвратит те же документы, что и поисковый запрос `money information`, но вес слова `money` будет оцениваться поисковым сервером при сортировке результатов в пять раз выше, чем вес слова `information`.
##	Регулярное выражение	Регулярные выражения позволяют выполнять поиск сложных сочетаний различных символов. Регулярное выражение в поисковом запросе должно быть заключено в двойные кавычки и начинаться с оператора `##`. Поисковый сервер использует реализацию регулярных выражений на базе TR1 (подробнее см. в статье msdn.microsoft.com/ru-ru/library/bb982727.aspx). Регулярное выражение может соответствовать только одному слову или группе цифр, поиск нескольких слов невозможен. Преобразование регистра (заглавные/прописные буквы) не производится, так что регулярное выражение должно соответствовать регистру строковых данных, хранимых в индексе. Скорость поиска зависит от размещения регулярного выражения в поисковом запросе: чем ближе выражение к началу слова, тем больше времени занимает поиск.

Обзор логических операторов

Поисковый сервер позволяет использовать “булевские” поисковые запросы, в которых слова или выражения объединяются логическими операторами, такими как `AND` или `OR`. Примеры:

- price `AND` quality - Должны присутствовать оба слова.
- price `OR` quality - Должно присутствовать хотя бы одно из указанных слов.
- price `W/3` quality - Слово “price” должно присутствовать на расстоянии не более 3-х слов от слова “quality”.
- price `NOT W/3` quality - Слово “price” должно присутствовать на расстоянии более 3-х слов от слова “quality”.
- price `AND NOT` quality - Слово “price” должно присутствовать, в то время как слова “quality” быть не должно.

В случае нескольких операторов используйте скобки, чтобы избежать неоднозначности поискового запроса. Например, запрос `price AND quality OR quantity` может означать `(price AND quality) OR quantity` либо `price AND (quality OR quantity)`. Для достижения наилучших результатов выражения с логическими операторами всегда следует заключать в скобки.

Поддерживаются следующие логические операторы:

- Операторы AND/OR
- Операторы W/N и PRE/N
- Операторы NOT и NOT W/N

Операторы AND/OR

Оператор `AND` используется для объединения двух слов или выражений, оба из которых должны присутствовать в каждом результате поиска.

Оператор `OR` используется для объединения двух слов или выражений, хотя бы одно из которых должно присутствовать в каждом результате поиска.

Операторы W/N и PRE/N

Оператор `W/N` используется, чтобы указать, что одно слово или выражение должно встречаться на расстоянии не более N слов от другого. Например, запрос `price W/3 quality` вернет результаты, содержащие слово “price” в пределах 3-х слов от слова “quality”.

Оператор `PRE/N` действует аналогично оператору `W/N`, но этот оператор также указывает, что первое выражение должно предшествовать второму. Например, запрос `price PRE/3 quality` вернет результаты, содержащие слово “price” на расстоянии не более 3-х слов перед словом “quality”.

Во избежание неоднозначной интерпретации поискового запроса по крайней мере одно из двух выражений, объединенных оператором `W/N` или `PRE/N`, должно быть одним словом или фразой, либо группой слов и фраз, объединенных оператором `OR`.

Для обозначения первого слова элемента поиска предусмотрен идентификатор `xfirstword`. Совместно с оператором `W/N` этот идентификатор позволяет выполнять поиск определенных слов или выражений вблизи начала элемента. Например, запрос `price W/3 xfirstword` вернет результаты, содержащие слово “price” в пределах 3-х слов от первого слова в сообщении или файле.

Операторы NOT и NOT W/N

Оператор `NOT` используется в начале выражения, чтобы изменить значение выражения на противоположное. Это позволяет исключить из результатов поиска те элементы, которые соответствуют данному выражению.

Оператор `NOT` можно поместить в начало поискового запроса. В этом случае он изменяет значение всего запроса на противоположное. Например, запрос `NOT (price W/3 quality)` вернет результаты, не содержащие слово “price” в пределах 3-х слов от слова “quality”.

Если оператор `NOT` используется в промежутке между выражениями, его необходимо дополнить другим оператором (например, оператором `AND` или `OR`). Так, запрос `price AND NOT quality` вернет результаты, которые содержат слово “price” и не содержат слова “quality”.

Сочетание операторов `NOT` и `W/N` (что означает “not within”) можно использовать для поиска слова или выражения в отдалении от другого слова или выражения. Например, запрос `price NOT W/3 quality` вернет результаты, содержащие слово “price” на расстоянии более 3-х слов от слова “quality”. Обратите внимание, что в отличие от оператора `W/N` оператор `NOT W/N` не является симметричным, так что, например, запрос `price NOT W/3 quality` не совпадает с запросом `quality NOT W/3 price`.

Действия по выполнению поиска

Для настройки и выполнения поиска выполните следующие действия:

1. В дереве консоли выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Поисковый сервер** > **Страница поиска**.

   На панели сведений будет отображена страница поиска.

2. На странице поиска в поле **Поиск** задайте строку запроса на поиск требуемых слов или выражений.

   При составлении строки запроса можно использовать команды контекстного меню, появляющегося при щелчке правой кнопкой мыши в поле **Поиск**:

   - **Вставить текст** - Укажите на этот пункт меню, чтобы добавить в поле **Поиск** логический оператор, сохраненную строку запроса или контентно-зависимую группу поиска:

     - Добавить логический оператор - Оператор `AND`, `OR` и т.п. можно ввести с клавиатуры в верхнем регистре или выбрать из меню **Вставить текст**. Подробнее см. в разделе Обзор логических операторов.

     - Добавить сохраненный запрос - Команда **Сохраненный запрос** позволяет добавить ранее сохраненную строку запроса. Подробнее о сохраненных запросах см. в разделе Управление сохраненными запросами.

     - Добавить группу поиска - Команда **Контентно-зависимая группа** позволяет добавить контентно-зависимую группу поиска. Подробнее о группах поиска см. в разделе Управление контентно-зависимыми группами поиска.

       В поле **Поиск** группа поиска представлена ее именем, заключенным в знаки процента: `%имя_группы%`. Группу поиска можно добавить, введя в это поле знак процента и имя группы.

   - **Сохранить как** - Сохранить текущую строку запроса для дальнейшего повторного использования. Подробнее см. в разделе Управление сохраненными запросами.

3. Чтобы задать параметры поиска, нажмите кнопку **Параметры** и выполните следующие действия:

   - Чтобы задать количество результатов поиска, возвращаемых на страницу, в списке **Отображать** <число> **результатов на странице** выберите один из следующих вариантов: **10**, **20**, **30**, **50**, **100**. По умолчанию возвращается 20 результатов.

   - Для поиска только в определенных журналах, установите соответствующие флажки в области **Результаты только из следующих журналов**.

     По умолчанию для поиска выбраны журнал аудита, журнал теневого копирования и журнал удаленных данных теневого копирования.

- Для поиска записей по дате задайте желаемый диапазон, используя следующие параметры:
  - **С** - Определяет начальную дату диапазона. Возможные значения:
    - **Первой записи** - Поиск записей, начиная с самой ранней в журнале. Это значение выбрано по умолчанию.
    - **Записи от** - Поиск записей, зарегистрированных в журнале после определенной даты.
  - **По** - Определяет конечную дату диапазона. Возможные значения:
    - **Последнюю запись** - Поиск записей до самой поздней в журнале. Это значение выбрано по умолчанию.
    - **Записи от** - Поиск записей, зарегистрированных в журнале до определенной даты.

  Если выбрано значение **Записи от**, щелкните в поле **С** или **По**, чтобы открыть календарь. В календаре щелчком мыши выберите требуемую дату. Используйте стрелки **<** | **>** для выбора месяца и двойные стрелки **<<** | **>>** для выбора года.
- Для поиска записей по отправителю, получателю, типу файла, типу устройства или протоколу, используйте параметры, представленные в области **Результаты, удовлетворяющие условиям**:
  - **Отправители** - Идентификаторы отправителей для следующих протоколов: IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMTP, Telegram, Viber, Web-почта, WhatsApp, Zoom. Поиск возвращает записи, связанные с указанными отправителями.
  - **Получатели** - Идентификаторы получателей для протоколов IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMTP, Telegram, Viber, Web-почта, WhatsApp, Zoom, а также следующих социальных сетей: Facebook, Google+, LiveJournal, LinkedIn, LiveInternet, Myspace, Odnoklassniki, Twitter, VKontakte. Поиск возвращает записи, связанные с указанными получателями.
  - **Типы файлов** - Описание типов искомых файлов (полное или частичное), например: “E-Mail message (Var.2)”, “Disk Image (Macintosh)”, “Zip 1.0”. Поиск возвращает записи, связанные с указанными типами файлов.
  - **Источники** - Искомые типы устройств или протоколы. Поиск возвращает записи, связанные с устройствами указанных типов или указанными протоколами.

  В полях **Отправители**, **Получатели** и **Типы файлов** допускается использование звездочки (*) для обозначения любого ряда символов и вопросительного знака (?) для обозначения любого одиночного символа, а также использование логических операторов `AND` (пробел) и `OR` (точка с запятой ;).

4. Нажмите кнопку **Поиск**.

Управление сохраненными запросами

При выполнении полнотекстового поиска или настройке поисковой задачи необходимо задать строку запроса на поиск определенных слов или фрагментов текста. Поскольку создание такой строки "с чистого листа" может отнимать много времени, имеется возможность сохранения и повторного использования поисковых запросов.

Строку запроса можно сохранить из поля **Поиск** (см. Действия по выполнению поиска): Щелкните правой кнопкой мыши в поле **Поиск**, выберите **Сохранить как** и укажите имя запроса в появившемся диалоговом окне. Другой способ открыть это окно: Щелкните правой кнопкой мыши в поле **Поиск**, укажите на **Вставить текст** и выберите **Сохраненный запрос**.

Строку запроса можно также сохранить из поля **Запрос** поисковой задачи (см. Настройка поискового запроса). Для этого щелкните правой кнопкой мыши в поле **Запрос**, выберите **Сохранить как** и укажите имя запроса в появившемся диалоговом окне. Другой способ открыть это окно: Нажмите кнопку **Сохраненный запрос** рядом с полем **Запрос**.

Диалоговое окно для управления сохраненными запросами отображает список всех доступных сохраненных запросов и позволяет совершать следующие действия:

- **Создать и сохранить новый запрос** - Нажмите кнопку **Новый** и задайте строку запроса аналогично тому, как это делается при настройке запроса поисковой задачи или полнотекстового поиска.
- **Просмотреть или изменить запрос** - Выберите запрос из списка и нажмите кнопку **Редактировать** для просмотра/изменения строки запроса.
- **Изменить имя запроса** - Выберите запрос и нажмите кнопку **Переименовать**.
- **Удалить запрос** - Выберите запрос и нажмите кнопку **Удалить**.
- **Экспортировать все сохраненные запросы в файл** - Нажмите кнопку **Сохранить** и затем укажите файл для хранения экспортированных запросов.
- **Импортировать запросы из файла** - Нажмите кнопку **Загрузить** и выберите файл, в котором хранятся экспортированные запросы.

Создание или редактирование сохраненного запроса

При создании, просмотре или изменении сохраненного запроса появляется диалоговое окно для управления данным запросом.

В поле **Запрос** этого диалогового окна укажите одну или несколько строк запроса на поиск требуемых слов или фрагментов текста, аналогично тому, как это делается при настройке поисковой задачи или выполнении полнотекстового поиска. Строки в запросе объединяются логическим оператором `AND`, так что поиск вернет результаты, которые содержат каждую из указанных строк.

В строке запроса можно использовать логические операторы, такие как `AND` или `OR`, вводя их с клавиатуры в верхнем регистре или выбирая оператор из контекстного меню. Чтобы открыть меню, щелкните правой кнопкой мыши в поле **Запрос** и укажите на пункт **Вставить текст**, или щелкните в поле **Запрос** и нажмите комбинацию клавиш Ctrl+D. Описание операторов см. в разделе Обзор логических операторов.

Строка запроса может содержать группы поиска (см. Управление контентно-зависимыми группами поиска). Для представления такой группы в поле **Запрос** служит имя, заключенное в знаки процента: `%имя_группы%`. Группу можно добавить в строку запроса, введя знак процента и имя. По мере ввода в поле **Запрос** появляется список групп, имена которых соответствуют введенному имени. Группу можно выбрать из этого списка.

Контекстное меню поля **Запрос** содержит также стандартные команды для работы с текстом, такие как **Вырезать**, **Копировать**, **Вставить** и т.п.

Управление контентно-зависимыми группами поиска

Контентно-зависимые группы поиска позволяют выполнять поиск записей журналов и других объектов данных по различным признакам, таким как типы файлов, ключевые слова, свойства документа и т.п. Группы поиска аналогичны контентным группам, которые используются контентно-зависимыми правилами в сервисе DeviceLock и правилами обнаружения контента в сервере Discovery. Как и контентные группы, группы поиска служат для определения искомых данных. Запрос, содержащий группу поиска, возвращает результаты, соответствующие этой группе.

Группы поиска создаются и хранятся отдельно от поисковых запросов. Этим обеспечивается централизованное управление группами поиска с возможностью их повторного использования в различных запросах и задачах. При администрировании групп поиска нужно учитывать, что изменение какой-либо группы поиска влияет на результаты всех поисковых запросов и задач, основанных на этой группе.

Группы поиска сохраняются в базе данных сервера DeviceLock Content Security Server на SQL-сервере. В консоли DeviceLock Management Console хранилище этих групп называется “база данных контента”. Поскольку группы поиска хранятся на SQL-сервере, база данных контента может не зависеть от консоли и сервера DeviceLock, использующего эту базу данных.

Группы поиска можно добавлять в запросы полнотекстового поиска (см. Действия по выполнению поиска), а также в запросы поисковых задач (см. Настройка поискового запроса).

В перечисленных ниже разделах приводятся инструкции по управлению группами поиска, а также описание групп поиска и их параметров по типам групп:

- Диалоговое окно управления группами поиска - Выбор, просмотр, создание и настройка контентно-зависимых групп поиска.
- Группы определения типа файла - Поиск файлов по значению поля “Тип файла”.
- Группы ключевых слов - Поиск указанных ключевых слов или фраз в файлах/данных.
- Группы шаблонов - Поиск фрагментов текста при помощи регулярных выражений.
- Группы свойств документа - Поиск документов с определенными свойствами (например, имя документа, его заголовок, тема и т.п.).
- Составные группы - Построение логического выражения из групп различных типов.

Диалоговое окно управления группами поиска

Диалоговое окно управления группами поиска появляется, если выбрать команду **Контентно-зависимая группа** из меню **Вставить текст** в поле **Поиск** на странице поиска (см. Действия по выполнению поиска) или нажать кнопку **База данных контента** рядом с полем **Запрос** на странице настройки запроса поисковой задачи (см. Настройка поискового запроса).

Диалоговое окно отображает список групп из базы данных контента поискового сервера. Для каждой группы в списке приводится ее имя и тип, а также флажок **Индексируется**. Список можно отфильтровать, выбрав нужный тип в поле **Отображать** под списком групп. Список содержит только группы того типа, который выбран в поле **Отображать**.

Флажок **Индексируется** влияет только на группы шаблонов и на составные группы, в которых имеются группы шаблонов. Для других типов групп он всегда установлен и не может быть снят. Установка этого флажка у какой-либо группы шаблонов/составной группы приводит к появлению в поисковом индексе дополнительной информации с целью обеспечить данной группе следующие дополнительные возможности поиска:

- Использование регулярных выражений для поиска фрагментов текста, состоящих из нескольких слов или нескольких групп цифр, разделенных пробелами или знаками препинания. Без флажка **Индексируется** группа способна находить только отдельные слова или последовательности цифр.
- Параметры поиска **Проверка**, **Учитывать регистр**, **Учитывать визуально похожие символы** и **Кириллическая транслитерация** (их описание см. в разделе Настройка, просмотр или изменение группы шаблонов). Без флажка **Индексируется** эти параметры не действуют.
- Символы ^ и $ для соответствия началу и концу строки. Если флажок **Индексируется** не установлен, в поисковом индексе нет сведений о переходе на новую строку, поэтому выражения, содержащие символ начала и/или конца строки (^ и $), работать не будут.

После установки флажка **Индексируется** дополнительные возможности поиска становятся доступными только для вновь проиндексированных данных. Чтобы распространить их на ранее проиндексированные данные, необходимо создать новый индекс. Следуйте инструкции в разделе Построение нового индекса по запросу и нажмите кнопку **Да** в окне сообщения о подтверждении операции, чтобы создать новый индекс взамен существующего (это может занять много времени).

Внимание:

- Установка флажка **Индексируется** может в несколько раз увеличить время построения поискового индекса.
- Для групп, которым не требуются дополнительные возможности поиска, флажок **Индексируется** установлен по умолчанию и не может быть снят. Это не влияет на время построения индекса.
- Дополнительные возможности поиска не распространяются на данные, которые были ранее проиндексированы, но отсутствуют на сервере во время создания нового индекса после установки флажка **Индексируется** (например, копии документов, удаленные из журнала теневого копирования).

В диалоговом окне управления группами поиска можно выполнить следующие действия:

- Добавить одну или несколько групп в поисковый запрос. Выберите требуемые группы в списке и нажмите кнопку **Добавить** или дважды щелкните требуемую группу.
- Создать новую группу или просмотреть/изменить параметры существующей группы:
  - Чтобы создать новую группу, используя настройки по умолчанию, нажмите стрелку рядом с кнопкой **Добавить группу** и выберите нужный тип группы.
  - Чтобы создать новую группу, используя настройки другой, уже существующей группы, выберите эту группу в списке и нажмите кнопку **Дублировать**.

    Примечание: Дублирование часто используется для создания редактируемых копий встроенных групп.

  - Чтобы просмотреть или изменить параметры существующей группы, выберите эту группу в списке и нажмите кнопку **Редактировать группу** (для групп, созданных администратором) или кнопку **Просмотр группы** (для встроенных групп, изменение которых не допускается).

  В результате любого из этих действий появляется диалоговое окно, в котором можно задать, просмотреть или изменить параметры группы.
- Удалить группу, ранее созданную администратором. Выберите группу в списке и нажмите кнопку **Удалить группу**. Для встроенных групп эта кнопка недоступна, поскольку удалять такие группы запрещено.

При создании, дублировании, просмотре или редактировании группы в консоли используется единое диалоговое окно для управления параметрами групп данного типа. Эти параметры для каждого типа групп описаны в следующих разделах:

- Группы определения типа файла
- Группы ключевых слов
- Группы шаблонов
- Группы свойств документа
- Составные группы

Группы определения типа файла

Группы определения типа файла служат для поиска файлов определенного типа независимо от расширения имени файла. Например, с помощью такой группы можно находить теневые копии файлов указанных типов. Группа позволяет указать один или несколько типов файлов. Поиск выполняется по значению поля “Тип файла”, присвоенному файлам в журналах DeviceLock. В результате сервер возвращает файлы, у которых значение этого поля соответствует любому из указанных в группе типов.

Поисковый сервер предоставляет широкий выбор предопределенных (встроенных) групп определения типа файла. Можно использовать встроенные группы в их исходном виде, создавать их дубликаты (редактируемые копии) или создавать новые группы для решения частных задач организации. Встроенные группы облегчают задачу настройки поисковых запросов, позволяя во многих случаях обойтись без создания новых групп. Для получения дополнительной информации см. список встроенных групп определения типа файла.

Для встроенных групп данного типа можно только просматривать списки их файловых типов в описанном ниже диалоговом окне. Изменение встроенных групп не допускается. Если нужно изменить типы файлов у встроенной группы, необходимо создать ее редактируемую копию путем дублирования группы (см. Диалоговое окно управления группами поиска).

Настройка, просмотр или изменение группы определения типа файла

При создании, дублировании, просмотре или редактировании группы определения типа файла (см. Диалоговое окно управления группами поиска) используется диалоговое окно, состоящее из двух панелей:

- **Группа контента** - На левой панели под этим заголовком перечисляются типы файлов, включенные в данную группу. Для каждого типа приводятся возможные расширения имени файла и дается краткое описание данного типа. Группа служит для поиска файлов указанных здесь типов. Во время поиска типы файлов объединяются по ИЛИ, т.е. файл соответствует группе, если его тип совпадает с любым из перечисленных.

  Поле **Имя** над списком типов позволяет задать, просмотреть или изменить имя группы.

- **Доступный контент** - На правой панели под этим заголовком перечисляются типы файлов, которые можно выбрать для включения в группу. Для каждого типа приводятся возможные расширения имени файла и дается краткое описание данного типа.

  Примечание: При просмотре группы данная панель не отображается.

  Поле над списком **Доступный контент** служит для поиска желаемых типов. Введите в это поле строку поиска и затем выполните поиск или фильтрацию:

  - Нажмите кнопку **Найти** или **Найти предыдущее** для поиска расширений имени файла или описаний файловых типов, в которых встречается данная строка.

    Нажимайте **Найти** для перехода к следующему вхождению строки поиска в списке. Нажимайте **Найти предыдущее**, чтобы вернуться к предыдущему вхождению этой строки.

  - Нажмите кнопку **Фильтр**, чтобы оставить в списке только те типы файлов, у которых данная строка поиска встречается в расширениях имени файла или описании типа.

  В строке поиска можно использовать звездочку (*) для обозначения произвольной последовательности символов и знак вопроса (?) для обозначения любого одиночного символа.

Кнопки в промежутке между панелями диалогового окна предназначены для добавления или удаления файловых типов из данной группы:

< - Выберите типы файлов на правой панели и нажмите кнопку <, чтобы добавить их в группу. Выбранные типы файлов будут добавлены в список на левой панели.

> - Выберите типы файлов на левой панели и нажмите кнопку >, чтобы удалить их из группы. Выбранные типы файлов будут удалены из списка на левой панели.

>> - Нажмите эту кнопку, чтобы удалить все типы файлов из группы. Нажатие кнопки >> очищает список на левой панели.

<< - Нажмите эту кнопку, чтобы добавить в группу все доступные типы файлов. Нажатие кнопки << добавляет в список на левой панели все типы файлов, перечисленные на правой панели.

Примечание: При просмотре группы эти кнопки не отображаются.

Группы ключевых слов

Группы ключевых слов позволяют находить записи журналов и объекты данных (например, файлы, электронные письма или мгновенные сообщения) по заданным словам и/или выражениям - так называемым "ключевым словам". Например, с помощью групп данного типа можно находить теневые копии файлов или записи аудита, в которых встречаются заданные ключевые слова. В группе задают требуемые ключевые слова и параметры поиска (например, искать ли все ключевые слова или хотя бы одно из них). Затем выполняется поиск объектов, содержащих заданные в группе ключевые слова.

Поисковый сервер предоставляет широкий выбор предопределенных (встроенных) групп ключевых слов. Можно использовать встроенные группы в их исходном виде, создавать их дубликаты (редактируемые копии) или создавать новые группы для решения частных задач организации. Встроенные группы облегчают задачу настройки поисковых запросов, позволяя во многих случаях обойтись без создания новых групп. Для получения дополнительной информации см. список встроенных групп ключевых слов.

Для встроенных групп данного типа можно только просматривать их ключевые слова и другие параметры в описанном ниже диалоговом окне. Изменение встроенных групп не допускается. Если нужно изменить ключевые слова у встроенной группы, следует создать ее редактируемую копию путем дублирования группы (см. Диалоговое окно управления группами поиска).

Настройка, просмотр или изменение группы ключевых слов

При создании, дублировании, просмотре или редактировании группы ключевых слов (см. Диалоговое окно управления группами поиска) используется диалоговое окно со следующими полями управления параметрами группы:

- **Имя**, **Описание** - Задать, просмотреть или изменить имя и описание группы.
- **Условие** - Просмотреть или выбрать условие поиска:
  - **Совпадение по любым ключевым словам** - Группа ищет объекты, которые содержат хотя бы одно из ее ключевых слов.
  - **Совпадение по всем ключевым словам** - Группа ищет объекты, которые содержат каждое из ее ключевых слов.
- **Ключевые слова** - Просмотреть или изменить ключевые слова данной группы:
  - Чтобы добавить ключевое слово, нажмите кнопку **Добавить** под списком ключевых слов, а затем введите нужное слово или фразу. По завершении нажмите клавишу Enter.
  - Чтобы изменить ключевое слово, уже имеющееся в списке, дважды щелкните в поле **Ключевые слова** и введите необходимые изменения. По завершении нажмите клавишу Enter.
  - Чтобы удалить ключевые слова, выберите их в списке и нажмите кнопку **Удалить** под списком ключевых слов.
  - Чтобы добавить ключевые слова из текстового файла, нажмите кнопку **Загрузить** под списком ключевых слов и откройте файл в появившемся диалоговом окне. Каждое ключевое слово в этом файле должно располагаться на отдельной строке с переходом на новую строку после последнего символа ключевого слова.

В списке ключевых слов можно просмотреть или изменить следующий параметр поиска индивидуально для каждого ключевого слова:

- **Целое слово** - Определяет, следует ли искать только такие объекты, где ключевое слово встречается в виде отдельного слова, а не в составе другого слова. Если флажок **Целое слово** установлен, выполняется поиск слова, в точности совпадающего с данным ключевым словом (например, поиск по ключевому слову `тест` не обнаружит слово `тесто` или `протест`). Если этот флажок снят, ищутся также слова, содержащие данное ключевое слово (`тесто` и `протест` в таком случае окажутся в результатах поиска наряду со словом `тест`).

Группы шаблонов

Группы шаблонов позволяют находить записи журналов и объекты данных (например, файлы, электронные письма или мгновенные сообщения) путем сопоставления их текстового содержимого с регулярными выражениями - так называемыми “шаблонами”. Регулярные выражения дают возможность поиска сложно устроенных комбинаций символов, таких как номера кредитных карт, номера социального страхования, адреса электронной почты, номера телефонов и т.п. В группах шаблонов используются регулярные выражения на языке Perl, описанные в документации по адресу perldoc.perl.org/perlrequick.html и perldoc.perl.org/perlretut.html.

С помощью таких групп можно находить, например, теневые копии, в которых встречаются строки, соответствующие определенным регулярным выражениям. В группе шаблонов задают регулярные выражения и другие параметры поиска (см. Настройка, просмотр или изменение группы шаблонов), а затем сервер выполняет поиск объектов, соответствующих регулярным выражениям из этой группы.

Поисковый сервер предоставляет широкий выбор предопределенных (встроенных) групп шаблонов. Можно использовать встроенные группы в их исходном виде, создавать их дубликаты (редактируемые копии) или создавать новые группы для решения частных задач организации. Встроенные группы облегчают задачу настройки поисковых запросов, позволяя во многих случаях обойтись без создания новых групп. Для получения дополнительной информации см. список встроенных групп шаблонов.

Для встроенных групп данного типа можно только просматривать их регулярные выражения и другие параметры в описанном ниже диалоговом окне. Изменение встроенных групп не допускается. Если нужно изменить встроенную группу, следует создать ее редактируемую копию путем дублирования группы (см. Диалоговое окно управления группами поиска).

Настройка, просмотр или изменение группы шаблонов

При создании, дублировании, просмотре или редактировании группы шаблонов (см. Диалоговое окно управления группами поиска) используется диалоговое окно со следующими полями управления параметрами группы:

- **Имя**, **Описание** - Задать, просмотреть или изменить имя и описание группы.
- **Выражение** - Просмотреть, добавить или изменить регулярные выражения для данной группы. В поле **Выражение** можно ввести одно или несколько выражений, по одному выражению на строку. Подробнее о регулярных выражениях см. в руководствах “Perl regular expressions quick start” по адресу perldoc.perl.org/perlrequick.html и “Perl regular expressions tutorial” по адресу perldoc.perl.org/perlretut.html.

  При сопоставлении объекта данных с группой во время поиска сервер подсчитывает общее количество совпадений данных с выражениями, указанными в этом поле, и определяет, соответствует ли объект группе, в зависимости от выбранного условия поиска (см. ниже).
- **Проверить** - Проверить синтаксис регулярного выражения.
- **Проверка** - Если настроена проверка, то соответствие данных группе обнаруживается только в случае их соответствия выбранному типу проверки. Чтобы соответствовать группе, данные должны соответствовать регулярному выражению, а также пройти проверку.

  Если для этого поля выбран вариант **Без проверки**, то для соответствия данных группе достаточно их соответствия регулярному выражению.

  Чтобы настроить проверку, выберите нужный тип из выпадающего списка в этом поле.
- **Учитывать регистр** - Если этот флажок установлен, группа различает строчные и прописные буквы. Например, слова `Серия` и `серия` в этом случае считаются разными словами, так что группе может соответствовать слово `Серия`, но не `серия`.

  Если этот флажок снят, группа не различает прописные и строчные буквы. В этом случае, если такой группе соответствует слово `Серия`, то ей будут соответствовать также слово `серия` и даже слово `сЕрИя`.

- **Учитывать визуально похожие символы** - Если этот флажок установлен, группа обнаруживает данные, которые соответствуют ее выражению, даже в случае замены отдельных символов на другие, сходные по внешнему виду или значению, в том числе:
  - Латинские буквы в русском тексте (например, латинская буква `b` вместо русской буквы `ь`)
  - Латинские буквы вместо некоторых цифр (например, латинская буква `S` вместо цифры `5`)
  - Русские буквы в английском тексте (например, русская буква `п` вместо латинской буквы `n`)
  - Русские буквы вместо некоторых цифр (например, русская буква `З` вместо цифры `3`)
  - Некоторые символы вместо русских букв (например, символ `*` (звездочка) вместо русской буквы `ж`)
  - Цифры вместо некоторых латинских или русских букв (например, цифра `1` вместо латинской буквы `I` или цифра `4` вместо русской буквы `Ч`)
  - Индо-арабские (восточно-арабские) цифры вместо обычных арабских цифр (например, символ `٣` вместо цифры `3` или символ `٨` вместо цифры `8`)

  Если этот флажок снят, группа строго различает символы независимо от того, похожи они или нет по внешнему виду или значению.
- **Кириллическая транслитерация** - Если этот флажок установлен, группа распознает кириллический текст, подлежащий обнаружению, независимо от того, написан ли текст кириллицей или латинскими буквами. Например, если слово `Серия` соответствует такой группе, то слово `Seriya` также будет ей соответствовать.

  Если этот флажок снят, соответствие текста группе строго зависит от алфавита, используемого для написания текста. Например, такой группе может соответствовать слово `Серия`, но не `Seriya`.
- **Дополнительно** - Проверить регулярное выражение на пробном тексте. Нажмите кнопку **Дополнительно**, чтобы отобразить или скрыть поле **Тестовый пример**.
- **Тестовый пример** - Ввести текстовую строку для проверки и просмотреть результат. Результаты проверки выделяются цветом в режиме реального времени. Зеленым цветом отображаются все соответствия регулярному выражению группы, а последовательности символов, не соответствующие этому выражению, отображаются красным цветом.

Внимание:

- Чтобы обеспечить группе шаблонов дополнительные возможности поиска, для нее необходимо установить флажок **Индексируется** (см. Диалоговое окно управления группами поиска). В противном случае группа будет способна находить только отдельные слова или последовательности цифр, и, кроме того, следующие параметры группы могут не действовать или работать неправильно: **Проверка**; **Учитывать регистр**; **Учитывать визуально похожие символы**; **Кириллическая транслитерация**.
- Для групп шаблонов, которым не требуются дополнительные возможности поиска, флажок **Индексируется** установлен по умолчанию и не может быть снят.
- После обновления DeviceLock может потребоваться пересоздать поисковый индекс, чтобы обеспечить поиск адресов электронной почты и номеров кредитных карт по данным, которые были проиндексированы старой версией DeviceLock. Для создания нового индекса следуйте инструкции, приведенной в разделе Построение нового индекса по запросу, и нажмите кнопку **Да** в окне запроса на подтверждение, чтобы заменить существующий индекс новым.
- Встроенная группа шаблонов **Номер кредитной карты** не позволяет находить записи журналов и объекты данных, содержащие номера кредитных карт платежной системы МИР. Для поиска таких данных создайте и используйте дубликат встроенной группы **Номер кредитной карты**.

Группы свойств документа

Группы свойств документа позволяют находить объекты данных (например, документы, электронные письма или мгновенные сообщения) по различным параметрам, которые можно получить из журналов DeviceLock. Эти параметры - так называемые “свойства документа” - перечислены и описаны ниже в разделе Настройка, просмотр или изменение группы свойств документа. С помощью группы свойств документа можно, например, находить теневые копии документов с определенными значениями таких свойств как Заголовок, Тема, Категории, Сохранен и т.п. В группе задают значения свойств искомых документов, после чего можно выполнять поиск документов, свойства которых соответствуют этой группе.

Настройка, просмотр или изменение группы свойств документа

При создании, дублировании, просмотре или редактировании группы свойств документа (см. Диалоговое окно управления группами поиска) используется диалоговое окно со следующими полями управления параметрами группы:

- **Имя**, **Описание** - Задать, просмотреть или изменить имя и описание группы.
- **Имя файла** - Задать, просмотреть или изменить имена искомых файлов. Если задан этот параметр, выполняется поиск файлов, имеющих любое из указанных имен.

  Чтобы указать несколько имен, используйте точку с запятой (;) в качестве разделителя. В имени файла можно использовать звездочку (*) для обозначения произвольной группы символов и знак вопроса (?) для обозначения одного произвольного символа.
- **Размер** - Задать, просмотреть или изменить размер искомых файлов в байтах, килобайтах (KB), мегабайтах (MB), гигабайтах (GB) или терабайтах (TB). Если задан этот параметр, выполняется поиск файлов, соответствующих выбранному варианту размера.

  Предусмотрены следующие параметры размера:

  - **Не указан** (выбрано по умолчанию) - Поиск файлов произвольного размера.
  - **Равен** - Поиск файлов, размер которых равен указанному.
  - **Меньше чем** - Поиск файлов, размер которых меньше указанного.
  - **Больше чем** - Поиск файлов, размер которых больше указанного.
  - **Между** - Поиск файлов, размер которых находится в указанном диапазоне.

  Внимание: После обновления DeviceLock может потребоваться пересоздать поисковый индекс, чтобы обеспечить поиск на основе размера файлов по данным, которые были проиндексированы старой версией DeviceLock. Для создания нового индекса следуйте инструкции, приведенной в разделе Построение нового индекса по запросу, и нажмите кнопку **Да** в окне запроса на подтверждение, чтобы заменить существующий индекс новым.
- **Защищен паролем** - Установите этот флажок для поиска теневых копий защищенных документов. Если этот флажок установлен, поиск возвращает только документы со статусом “Да” в поле **Защищен** соответствующей записи журнала. Если флажок снят, значение этого поля не учитывается во время поиска.
- **Дополнительные параметры** - Настроить поиск, учитывающий свойства документов, такие как встроенные и настраиваемые (пользовательские) свойства документов Microsoft Office и документов других типов; классификационные метки сторонних продуктов, таких как Boldon James Classifier; отправителей и получателей мгновенных сообщений и электронных писем; имена устройств и протоколов для объектов поиска.

Предусмотрены следующие дополнительные параметры:

- **Заголовок**, **Тема**, **Теги**, **Компания**, **Менеджер**, **Комментарии**, **Авторы**, **Категории**, **Сохранен** - Задать, просмотреть или изменить значения, отвечающие некоторым часто используемым свойствам документов, которые требуется найти. Поддерживаются свойства документов MS Office (.docx, .xlsx, .pptx, .vsdx), .pdf и составных документов. Заголовок поля соответствует имени свойства, указанному в приложениях для работы с документами (например, MS Office Word или Adobe Acrobat).

  В этих полях можно использовать звездочку (*) для обозначения произвольной группы символов и знак вопроса (?) для обозначения одного произвольного символа. Нескольких значений в одно и то же поле можно ввести, разделяя их точкой с запятой (;). Пример ввода двух значений со знаками подстановки: `*Отчет*; *Счет*`.

  Значения, введенные в разных полях, объединяются по И. Если в одном поле введено несколько значений, они объединяются по ИЛИ.

  Полезный совет: Для поиска файлов с произвольным непустым значением какого-либо из этих свойства документа используйте маску `?*`. Звездочка без вопросительного знака соответствует любому значению свойства, а также его отсутствию.

- **Прочие и классификационные поля** - Просмотреть или ввести значения, отвечающие различным встроенным и настраиваемым (пользовательским) свойствам искомых документов. Поддерживаются свойства документов MS Office (.docx, .xlsx, .pptx), .pdf и составных документов.

  Чтобы ввести одно значение для некоторого свойства, используйте следующий синтаксис: `<имя свойства>=<значение свойства>`. Например, запись `Division=Sales` представляет значение Sales для свойства Division. Чтобы ввести несколько значений для одного и того же свойства, разделите их запятой. В этом случае значения объединяются по ИЛИ. Так, запись `Division=Sales,Finance` представляет значение Sales ИЛИ значение Finance для свойства Division.

  Чтобы ввести значения для нескольких свойств, разделите записи свойств точкой с запятой. Пример: `<имя1>=<значение11>,<значение12>; <имя2>=<значение21>`. Значения различных свойств объединяются по И, тогда как различные значения одного и того же свойства объединяются по ИЛИ. Так, запись `Division=Sales,Finance; Office=Head Office` представляет значение Sales ИЛИ значение Finance для свойства Division И значение Head Office для свойства Office.

  Поле **Прочие и классификационные поля** позволяет также настроить группу для распознавания классификационных меток сторонних продуктов, таких как Boldon James Classifier, которые сохраняют значения своих меток в свойствах документа. Если меткой является точное значение некоторого свойства, то для ее распознавания можно использовать описанный выше синтаксис `<имя свойства>=<значение свойства>`. Какое именно значение какого свойства служит для обозначения метки определяется настройками стороннего продукта.

  Чтобы настроить группу для распознавания SISL-меток Boldon James Classifier, используется синтаксис, который указывает идентификатор элемента `uid` требуемой метки: `uid=<значение ID>`. Значение ID можно выяснить из XML-данных SISL-метки какого-либо классифицированного документа. Подробнее об этом см. в разделе Распознавание меток Boldon James Classifier.

  В поле **Прочие и классификационные поля** можно использовать точку с запятой (;) в качестве разделителя для ввода нескольких записей, обозначающих различные свойства документа и/или классификационные метки. Все записи, разделенные точкой с запятой, объединяются по И.

  Примечание: Для облегчения настройки в поле **Прочие и классификационные поля** запоминаются ранее вводившиеся записи с возможностью их выбора из раскрывающегося списка, которым снабжено это поле.

- **Отправители** - Задать, просмотреть или изменить идентификаторы отправителей для следующих протоколов: IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMTP, Telegram, Viber, Web-почта, WhatsApp, Zoom. Если задан этот параметр, группа выполняет поиск записей, связанных с любым из указанных отправителей.

  Чтобы указать несколько отправителей, используйте точку с запятой (;) в качестве разделителя. В идентификаторе отправителя можно использовать звездочку (*) для обозначения произвольной группы символов и знак вопроса (?) для обозначения одного произвольного символа.

- **Получатели** - Задать, просмотреть или изменить идентификаторы получателей для протоколов IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMTP, Telegram, Viber, Web-почта, WhatsApp, Zoom, а также следующих социальных сетей: Facebook, Google+, LiveJournal, LinkedIn, LiveInternet, Myspace, Odnoklassniki, Twitter, VKontakte. Если задан этот параметр, группа выполняет поиск записей, связанных с любым из указанных получателей.

  Чтобы указать несколько получателей, используйте точку с запятой (;) в качестве разделителя. В идентификаторе получателя можно использовать звездочку (*) для обозначения произвольной группы символов и знак вопроса (?) для обозначения одного произвольного символа.

- **Источники** - Просмотреть или выбрать из выпадающего списка искомые типы устройств или протоколы. Если задан этот параметр, группа выполняет поиск записей, связанных с любым из выбранных устройств или протоколов.

При использовании дополнительных параметров учитывайте следующее:

- Различные параметры объединяются по И, то есть группа распознает документ, если он соответствует каждому из настроенных параметров. Например, чтобы документ распознавался группой, у которой заданы значения параметров `Заголовок` и `Тема`, соответствующие значения должны быть как у свойства `Заголовок`, так и у свойства `Тема` документа. Если требуется объединить параметры по ИЛИ, можно использовать составную группу, добавив в нее по отдельной группе свойств документа для каждого параметра.
- Для одного и того же параметра можно задать несколько значений, разделяя их точкой с запятой. В таком случае значения объединяются по ИЛИ, так что группа распознает документ, если он соответствует любому из заданных значений. Так, если в параметре `Заголовок` указано `Отчет; Счет`, то группа распознает документы, у которых в свойстве `Заголовок` значится `Отчет` или `Счет`.

Составные группы

Составные группы позволяют объединять группы поиска с помощью логических выражений. Данные поиска соответствуют составной группе, если они удовлетворяют ее условию. Условие представляет собой логическое выражение, состоящее из одного или нескольких критериев. Каждый критерий использует некоторую группу поиска и принимает логическое значение `true`, если данные поиска соответствуют этой группе. В противном случае критерий принимает значение `false`. Значение выражения вычисляется из текущих значений его критериев, и данные считаются соответствующими составной группе при значении выражения равном `true`.

Настройка, просмотр или изменение составной группы

При создании, дублировании, просмотре или редактировании составной группы (см. раздел Диалоговое окно управления группами поиска) используется диалоговое окно, в котором можно добавлять и удалять критерии, объединять их по И/ИЛИ и группировать их с помощью скобок:

- Кнопки над списком критериев позволяют добавлять и удалять критерии, просматривать их поисковые группы, а также изменять порядок следования критериев в логическом выражении:
  - **Добавить** - Добавляет новый критерий в конец списка.

    Чтобы добавить новый критерий, нажмите кнопку **Добавить** или дважды щелкните пустую область в списке критериев.
  - **Вставить** - Добавляет новый критерий перед выбранным в списке.

    Для добавления критериев используется диалоговое окно, в котором можно выбрать одну или несколько групп. В условие добавляется по одному критерию для каждой из выбранных групп. Имя группы отображается в поле **Критерий**.
  - **Просмотр** - Открывает диалоговое окно для просмотра группы, выбранной в списке критериев. Это окно аналогично диалоговому окну для настройки групп соответствующего типа, в котором параметры группы доступны только для чтения.

    Для просмотра параметров группы нажмите кнопку **Просмотр** или дважды щелкните группу в списке критериев.
  - **Удалить** - Удаляет выбранный критерий, а также логические операторы и скобки, указанные вместе с этим критерием в списке.
  - **^**, **v** (стрелки вверх и вниз) - Перемещают выбранный критерий вверх или вниз по списку.

    Перемещение критериев вверх/вниз по списку может нарушить логическую структуру выражения. Нажмите кнопку **Проверить,** чтобы проверить синтаксис выражения и отобразить полученное выражение в поле **Результат**.
- Установите флажок в столбце **НЕ**, чтобы изменить возвращаемое критерием логическое значение на противоположное.
- Щелкните в столбце с заголовком **(** или **)**, чтобы добавить левые или правые скобки.

  Скобки позволяют избежать неоднозначности выражений из нескольких критериев. Например, выражение `А И В ИЛИ С` может означать `(А И В) ИЛИ С` либо `А И (В ИЛИ С)`. Используйте скобки, чтобы точно определить порядок вычисления выражений.

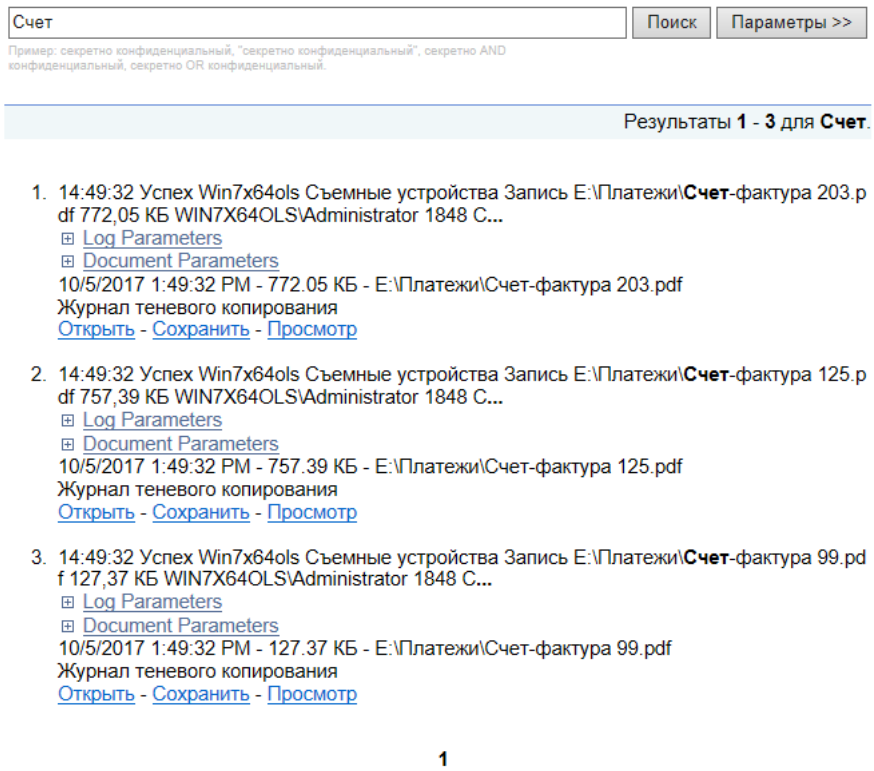
> **Примечание:** При перемещении какой-либо записи на место соседней в списке критериев флажок **НЕ** перемещается вместе с записью, только если количество открывающих скобок меньше или равно количеству закрывающих скобок как в перемещаемой записи, так и в записи, на место которой она перемещается. Если открывающих скобок хотя бы в одной из них больше, чем закрывающих, то этот флажок не переходит на соседнюю запись. Такое решение помогает сохранить логическую структуру выражения при изменении порядка записей в списке.

- Щелкните в столбце **И/ИЛИ**, чтобы выбрать оператор для объединения критериев в логическое выражение. По умолчанию выбран оператор **И**, так что данные поиска соответствуют группе, только если они соответствуют всем заданным критериям. Выберите оператор **ИЛИ**, если требуется, чтобы данные соответствовали группе при их соответствии хотя бы одному из этих критериев.
- **Проверить** - Проверяет синтаксис логического выражения, убирает заведомо лишние скобки, и отображает полученное выражение в поле **Результат**.
- **Очистить** - Удаляет все критерии из условия данной группы. В результате у группы отсутствует условие для поиска данных.

В диалоговом окне для настройки составных групп имеются также поля, позволяющие задать, просмотреть или изменить имя и описание группы.

Работа с результатами поиска

При выполнении полнотекстового поиска сервер возвращает страницу результатов поиска, которая выглядит следующим образом:



Страница результатов поиска разделена на несколько областей:

- Область запроса - Отображает заданные критерии поиска.
- Строка статистики - Показывает количество результатов поиска, отображенных на текущей странице результатов.
- Область результатов поиска - Отображает нумерованный список найденных результатов, соответствующих заданным критериям поиска.
- Навигатор результатов - Показывает количество страниц с результатами поиска и позволяет переходить с одной страницы на другую.

Каждая область подробно описана ниже.

Область запроса

Эта область расположена в верхней части страницы результатов поиска. Нажмите кнопку **Параметры**, чтобы посмотреть все заданные параметры поиска:

Поиск | Параметры <<

Пример: секретно конфиденциальный, "секретно конфиденциальный", секретно AND конфиденциальный, секретно OR конфиденциальный.

Отображать 20 результатов на странице

Результаты только из следующих журналов:

- ☑ Журнал аудита
- ☑ Журнал теневого копирования
- ☑ Журнал удаленных данных теневого копирования
- ☐ Журнал активности пользователей
- ☐ Журнал сервера
- ☐ Журнал мониторинга
- ☐ Журнал политик

Результаты только из следующего временного диапазона:

С: Первой зап...

По: Последнюю...

Результаты, удовлетворяющие условиям:

Отправители:

Получатели:

Типы файлов:

Источники:

Описание параметров поиска см. в разделе Действия по выполнению поиска.

Строка статистики

Эта область расположена непосредственно над результатами поиска и выглядит следующим образом:

Результаты **1** - **3** для **Счет**.

Область результатов поиска

Эта область расположена ниже области запроса и строки статистики и выглядит следующим образом:

1. 14:49:32 Успех Win7x64ols Съемные устройства Запись E:\Платежи**Счет**-фактура 203.pdf 772,05 КБ WIN7X64OLS\Administrator 1848 C...
   ⊞ Log Parameters
   ⊞ Document Parameters
   10/5/2017 1:49:32 PM - 772.05 КБ - E:\Платежи\Счет-фактура 203.pdf
   Журнал теневого копирования
   Открыть - Сохранить - Просмотр

2. 14:49:32 Успех Win7x64ols Съемные устройства Запись E:\Платежи**Счет**-фактура 125.pdf 757,39 КБ WIN7X64OLS\Administrator 1848 C...
   ⊞ Log Parameters
   ⊞ Document Parameters
   10/5/2017 1:49:32 PM - 757.39 КБ - E:\Платежи\Счет-фактура 125.pdf
   Журнал теневого копирования
   Открыть - Сохранить - Просмотр

Результат поиска содержит следующие элементы:

- **Фрагменты текста** - Отрывки текста, в которых встречаются слова, соответствующие поисковому запросу (выделены полужирным шрифтом). Эти фрагменты показывают, в каком контексте обнаружены искомые слова. В каждом результате поиска отображаются только первые три фрагмента текста.
- **Параметры журнала** - Сводная информация из журнала для данного результата поиска. Щелкните знак плюса (**+**), чтобы раскрыть область **Параметры журнала**. В зависимости от типа журнала в этой области предоставляется различная информация.

  Примечание: Пустые поля записей журнала не отображаются в области **Параметры журнала**.

  Для результатов поиска по журналу аудита в области **Параметры журнала** содержится следующая информация:

  - **Тип** - Тип события: **Успех** - действие разрешено; **Отказ** - действие запрещено; **Информация** - событие обнаружения контента; **Предупреждение** - сообщение о возможных осложнениях или ошибках. Соответствует данным столбца **Тип** в серверном просмотрщике журнала аудита.
  - **Компьютер** - Имя компьютера, на котором произошло событие. Соответствует данным столбца **Компьютер** в серверном просмотрщике журнала аудита.
  - **Дата/Время** - Дата и время, когда событие было получено сервисом DeviceLock. Соответствует данным столбца **Дата/Время** в серверном просмотрщике журнала аудита.
  - **Источник** - Тип устройства или протокол, вызвавший событие. Соответствует данным столбца **Источник** в серверном просмотрщике журнала аудита.
  - **Действие** - Действие пользователя. Соответствует данным столбца **Действие** в серверном просмотрщике журнала аудита.
  - **Имя** - Имя объекта (файла, USB-устройства и т.п.), связанного с событием. Соответствует данным столбца **Имя** в серверном просмотрщике журнала аудита.
  - **Информация** - Прочая относящаяся к устройству или протоколу информация о событии, такая как флаги доступа, имя устройства или протокола, ID и описание USB-устройства и т.п. Соответствует данным столбца **Информация** в серверном просмотрщике журнала аудита.
  - **Причина** - Причина возникновения события. Соответствует данным столбца **Причина** в серверном просмотрщике журнала аудита.
  - **Пользователь** - Имя пользователя, связанного с событием. Соответствует данным столбца **Пользователь** в серверном просмотрщике журнала аудита.
  - **PID** - Идентификатор процесса, связанного с событием. Соответствует данным столбца **PID** в серверном просмотрщике журнала аудита.
  - **Процесс** - Полный путь к исполняемому файлу приложения. В некоторых случаях вместо полного пути может быть показано только имя процесса. Соответствует данным столбца **Процесс** в серверном просмотрщике журнала аудита.
  - **Событие** - Номер, идентифицирующий событие. Соответствует данным столбца **Событие** в серверном просмотрщике журнала аудита.
  - **Дата/Время сбора** - Дата и время, когда событие было получено сервером DeviceLock Enterprise Server от сервиса DeviceLock. Соответствует данным столбца **Дата/Время сбора** в серверном просмотрщике журнала аудита.
  - **Сервер** - Имя сервера DeviceLock Enterprise Server, получившего событие от сервиса DeviceLock. Соответствует данным столбца **Сервер** в серверном просмотрщике журнала аудита.

- **Сервер консолидации** - Имя удаленного сервера, с которого событие было последний раз получено при консолидации журналов. Соответствует данным столбца **Сервер консолидации** в серверном просмотрщике журнала аудита.
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов. Соответствует данным столбца **Дата/Время консолидации** в серверном просмотрщике журнала аудита.
- **DeviceLock Enterprise Server** - Имя сервера DeviceLock Enterprise Server, с которого данные этого события были проиндексированы поисковым сервером.

Для результатов поиска по журналам теневого копирования и удаленных данных теневого копирования в области **Параметры журнала** содержится следующая информация:

- **Статус** - Состояние записи: **Успех** - теневая копия успешно создана; **Неполный** - возможно, теневая копия создана не полностью; **Отказ** - теневая копия данных, передача которых сопровождалась проверкой контентно-зависимыми правилами и была заблокирована на любом из уровней контроля. Соответствует данным столбца **Статус** в серверном просмотрщике журнала теневого копирования.
- **Компьютер** - Имя компьютера, с которого получена теневая копия. Соответствует данным столбца **Компьютер** в серверном просмотрщике журнала теневого копирования.
- **Дата/Время** - Дата и время записи теневой копии сервисом DeviceLock. Соответствует данным столбца **Дата/Время** в серверном просмотрщике журнала теневого копирования.
- **Источник** - Тип устройства или протокол, вызвавший событие. Соответствует данным столбца **Источник** в серверном просмотрщике журнала теневого копирования.
- **Действие** - Действие пользователя. Соответствует данным столбца **Действие** в серверном просмотрщике журнала теневого копирования.
- **Имя файла** - Оригинальное имя файла либо автоматически созданное имя для данных, которые изначально не были представлены в виде файла (такие как CD/DVD/BD-образ, данные записанные напрямую на носитель или переданные через COM или LPT-порт). Соответствует данным столбца **Имя файла** в серверном просмотрщике журнала теневого копирования.
- **Размер файла** - Размер данных. Соответствует данным столбца **Размер файла** в серверном просмотрщике журнала теневого копирования.
- **Тип файла** - Настоящий тип файла. Соответствует данным столбца **Тип файла** в серверном просмотрщике журнала теневого копирования.
- **Причина** - Причина возникновения события. Соответствует данным столбца **Причина** в серверном просмотрщике журнала теневого копирования.
- **Защищен** - Указывает состояние защиты файла. Соответствует данным столбца **Защищен** в серверном просмотрщике журнала теневого копирования.
- **Информация** - Прочая относящаяся к устройству или протоколу информация о событии, такая как флаги доступа, имя устройства или протокола, ID и описание USB-устройства и т.п. Соответствует данным столбца **Информация** в серверном просмотрщике журнала теневого копирования.
- **Пользователь** - Имя пользователя, передавшего данные. Соответствует данным столбца **Пользователь** в серверном просмотрщике журнала теневого копирования.
- **PID** - Идентификатор процесса приложения, использовавшегося для передачи данных. Соответствует данным столбца **PID** в серверном просмотрщике журнала теневого копирования.

- **Процесс** - Полный путь к исполняемому файлу приложения. В некоторых случаях вместо полного пути может быть показано только имя процесса. Соответствует данным столбца **Процесс** в серверном просмотрщике журнала теневого копирования.
- **Дата/Время сбора** - Дата и время, когда событие было получено сервером DeviceLock Enterprise Server от сервиса DeviceLock. Соответствует данным столбца **Дата/Время сбора** в серверном просмотрщике журнала теневого копирования.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, получившего событие от сервиса DeviceLock. Соответствует данным столбца **Сервер** в серверном просмотрщике журнала теневого копирования.
- **Сервер консолидации** - Имя удаленного сервера, с которого событие было последний раз получено при консолидации журналов. Соответствует данным столбца **Сервер консолидации** в серверном просмотрщике журнала теневого копирования.
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов. Соответствует данным столбца **Дата/Время консолидации** в серверном просмотрщике журнала теневого копирования.
- **DeviceLock Enterprise Server** - Имя сервера DeviceLock Enterprise Server, с которого данные этого события были проиндексированы поисковым сервером.

Для результатов поиска по журналу активности пользователей в области **Параметры журнала** содержится следующая информация:

- **Компьютер** - Имя компьютера, на котором был записан сеанс мониторинга пользовательской активности. Соответствует данным столбца **Компьютер** в серверном просмотрщике журнала активности пользователей.
- **Дата/Время** - Дата и время начала записи сеанса. Соответствует данным столбца **Дата/Время** в серверном просмотрщике журнала активности пользователей.
- **Тип** - Виды записи, доступные в данном сеансе: **Видеозапись** - Только запись экрана компьютера; **Запись клавиатуры** - Только запись нажатий клавиш на клавиатуре компьютера; **Видеозапись, Запись клавиатуры** - Запись экрана и запись нажатий клавиш. Соответствует данным столбца **Тип** в серверном просмотрщике журнала активности пользователей.
- **Правило** - Имя правила, вызвавшего запись. Здесь могут быть перечислены несколько правил, если во время данной записи сработало более одного правила. Соответствует данным столбца **Правило** в серверном просмотрщике журнала активности пользователей.
- **Причина** - Критерии запуска правила, которое вызвало запись. В случае нескольких правил для каждого из них отдельно перечисляются его критерии запуска. Соответствует данным столбца **Причина** в серверном просмотрщике журнала активности пользователей.
- **Продолжительность** - Промежуток времени, в течение которого выполнялась запись. Соответствует данным столбца **Продолжительность** в серверном просмотрщике журнала активности пользователей.
- **Пользователь** - Имя пользователя, активность которого записана в данном сеансе. Соответствует данным столбца **Пользователь** в серверном просмотрщике журнала активности пользователей.
- **Дата/Время сбора** - Дата и время, когда сервер DeviceLock Enterprise Server получил запись данного сеанса от сервиса DeviceLock. Соответствует данным столбца **Дата/Время сбора** в серверном просмотрщике журнала активности пользователей.

- **Сервер** - Имя компьютера, на котором работает сервер DeviceLock Enterprise Server, получивший запись данного сеанса от сервиса DeviceLock. Соответствует данным столбца **Сервер** в серверном просмотрщике журнала активности пользователей.
- **Сервер консолидации** - Имя удаленного сервера, с которого запись данного сеанса была последний раз получена при консолидации журналов. Соответствует данным столбца **Сервер консолидации** в серверном просмотрщике журнала активности пользователей.
- **Дата/Время консолидации** - Дата и время, когда запись данного сеанса была последний раз получена с удаленного сервера при консолидации журналов. Соответствует данным столбца **Дата/Время консолидации** в серверном просмотрщике журнала активности пользователей.
- **DeviceLock Enterprise Server** - Имя сервера DeviceLock Enterprise Server, с которого данные этого сеанса мониторинга были проиндексированы поисковым сервером.

Для результатов поиска по внутреннему журналу сервера DeviceLock Enterprise Server в области **Параметры журнала** содержится следующая информация:

- **Тип** - Тип события: **Успех**, **Информация**, **Предупреждение** или **Ошибка**. Соответствует данным столбца **Тип** в просмотрщике журнала сервера DeviceLock Enterprise Server.
- **Дата/Время** - Дата и время, когда событие произошло. Соответствует данным столбца **Дата/Время** в просмотрщике журнала сервера DeviceLock Enterprise Server.
- **Событие** - Номер, идентифицирующий событие. Соответствует данным столбца **Событие** в просмотрщике журнала сервера DeviceLock Enterprise Server.
- **Информация** - Прочая информация о событии, такая как описание ошибки, имя и значение измененного параметра и т.п. Соответствует данным столбца **Информация** в просмотрщике журнала сервера DeviceLock Enterprise Server.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, на котором событие произошло. Соответствует данным столбца **Сервер** в просмотрщике журнала сервера DeviceLock Enterprise Server.
- **Запись N** - Порядковый номер записи. Соответствует данным столбца **Запись N** в просмотрщике журнала сервера DeviceLock Enterprise Server.
- **Сервер консолидации** - Имя удаленного сервера, с которого событие было последний раз получено при консолидации журналов. Соответствует данным столбца **Сервер консолидации** в просмотрщике журнала сервера DeviceLock Enterprise Server.
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов. Соответствует данным столбца **Дата/Время консолидации** в просмотрщике журнала сервера DeviceLock Enterprise Server.
- **DeviceLock Enterprise Server** - Имя сервера DeviceLock Enterprise Server, с которого данные этого события были проиндексированы поисковым сервером.

Для результатов поиска по журналу мониторинга в области **Параметры журнала** содержится следующая информация:

- **Тип** - Тип события: **Успех**, **Информация**, **Предупреждение** или **Ошибка**. Соответствует данным столбца **Тип** в просмотрщике журнала мониторинга.
- **Дата/Время** - Дата и время, когда событие произошло. Соответствует данным столбца **Дата/Время** в просмотрщике журнала мониторинга.
- **Событие** - Номер, идентифицирующий событие. Соответствует данным столбца **Событие** в просмотрщике журнала мониторинга.

- **Имя задачи** - Имя задачи мониторинга, связанной с событием. Может быть пустым, если событие не имеет отношения к задачам мониторинга. Соответствует данным столбца **Имя задачи** в просмотрщике журнала мониторинга.
- **Имя компьютера** - Имя компьютера, который относится к связанной с событием задаче мониторинга. Может быть пустым, если событие не имеет отношения к компьютеру. Соответствует данным столбца **Имя компьютера** в просмотрщике журнала мониторинга.
- **Информация** - Прочая информация о событии, такая как описание ошибки, предупреждение и т.п. Соответствует данным столбца **Информация** в просмотрщике журнала мониторинга.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, на котором событие произошло. Соответствует данным столбца **Сервер** в просмотрщике журнала мониторинга.
- **Запись N** - Порядковый номер записи. Соответствует данным столбца **Запись N** в просмотрщике журнала мониторинга.
- **Сервер консолидации** - Имя удаленного сервера, с которого событие было последний раз получено при консолидации журналов. Соответствует данным столбца **Сервер консолидации** в просмотрщике журнала мониторинга.
- **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов. Соответствует данным столбца **Дата/Время консолидации** в просмотрщике журнала мониторинга.
- **DeviceLock Enterprise Server** - Имя сервера DeviceLock Enterprise Server, с которого данные этого событии были проиндексированы поисковым сервером.

Для результатов поиска по журналу политик сервера DeviceLock Enterprise Server в области **Параметры журнала** содержится следующая информация:

- **Тип** - Тип события: **Успех**, **Информация**, **Предупреждение** или **Ошибка**. Соответствует данным столбца **Тип** в просмотрщике журнала политик.
- **Дата/Время** - Дата и время, когда событие произошло. Соответствует данным столбца **Дата/Время** в просмотрщике журнала политик.
- **Событие** - Номер, идентифицирующий событие. Соответствует данным столбца **Событие** в просмотрщике журнала политик.
- **Объект политики** - Имя объекта политики, связанного с событием. Может быть пустым, если событие не имеет отношения к объектам политики. Соответствует данным столбца **Объект политики** в просмотрщике журнала политик.
- **Имя компьютера** - Имя компьютера, вызвавшего событие. Может быть пустым, если событие не связано с компьютером. Соответствует данным столбца **Имя компьютера** в просмотрщике журнала политик.
- **Информация** - Прочая информация о событии, такая как описание ошибки, предупреждение и т.п. Соответствует данным столбца **Информация** в просмотрщике журнала политик.
- **Сервер** - Имя сервера DeviceLock Enterprise Server, зарегистрировавшего событие. Соответствует данным столбца **Сервер** в просмотрщике журнала политик.
- **Запись N** - Порядковый номер записи. Соответствует данным столбца **Запись N** в просмотрщике журнала политик.

    - **Сервер консолидации** - Имя удаленного сервера, с которого событие было последний раз получено при консолидации журналов. Соответствует данным столбца **Сервер консолидации** в просмотрщике журнала политик.
    - **Дата/Время консолидации** - Дата и время, когда событие было последний раз получено с удаленного сервера при консолидации журналов. Соответствует данным столбца **Дата/Время консолидации** в просмотрщике журнала политик.
    - **DeviceLock Enterprise Server** - Имя сервера DeviceLock Enterprise Server, с которого данные этого события были проиндексированы поисковым сервером.
- **Параметры документа** - Сводная информация о свойствах документа из результата поиска по журналам теневого копирования. Щелкните знак плюса (**+**), чтобы раскрыть область **Параметры документа**. Эта область отображает различные сведения о документе в зависимости от его типа. Например, для теневой копии документа Word область **Параметры документа** отображает следующую информацию:
    - Приложение - Microsoft Office Word.
    - Автор - Имя пользователя, создавшего документ.
    - Создан - Дата и время создания документа.
    - Сохранен - Дата и время последнего сохранения документа.
    - Сохранен пользователем - Имя пользователя, сохранявшего документ последним.
    - Номер ревизии - Сколько раз документ был сохранен.
    - Шаблон - Имя шаблона документа.
    - Заголовок - Имя документа.
    - Время редактирования - Общее время правки в минутах.

  Для результатов поиска по журналу активности пользователей в области **Параметры документа** перечисляются введенные пользователем логины и пароли (если они были зарегистрированы в журнале). Параметр в данном случае называется `Пароли`.
- Дата и время записи в журнале.
- Размер записи в журнале. Это значение отображается только для теневых копий файлов, полученных из журнала теневого копирования.
- Имя журнала, в котором было найдено соответствие условиям поискового запроса.
- **Открыть**, **Сохранить**, **Просмотр** - На результатах поиска в журналах теневого копирования эти ссылки позволяют открывать, просматривать и сохранять теневые копии. Подробнее см. в разделе Работа с теневыми копиями.

  На результатах поиска в журнале активности пользователей эти ссылки используются, чтобы открыть, просмотреть или сохранить запись клавиатуры. Их нет на результатах поиска, не содержащих запись клавиатуры. Запись открывается в приложении, которое зарегистрировано для работы с HTML-файлами в операционной системе. При просмотре запись отображается в окне консоли. Сохранение записи выполняется в HTML-файл.

Примечание: Если поиск не дал результатов, на странице результатов поиска сообщается, что совпадений не найдено.

Навигатор результатов

Эта область расположена внизу страницы результатов поиска и выглядит следующим образом:

Предыдущее 1 2 **3** 4 5 6 7 8 9 10 11 12 Далее

Чтобы перемещаться по страницам результатов поиска, щелкните ссылку **Следующая** или **Предыдущая**, или щелкните номер страницы.

Работа с теневыми копиями

Консоль DeviceLock позволяет выполнить следующие операции с результатами поиска в журналах теневого копирования:

- Открыть теневую копию
- Сохранить теневую копию
- Открыть и сохранить теневую копию во встроенном средстве просмотра

Открыть теневую копию

Нажмите **Открыть** под нужным результатом поиска.

Теневая копия файла открывается в приложении, которое настроено для файлов данного типа на компьютере, где работает консоль DeviceLock. При отсутствии такого приложения, появится диалоговое окно "Открыть с помощью" для выбора приложения, с помощью которого следует открыть файл. Теневые копии файлов с устройств типа "Параллельный порт" открываются во программе просмотра DeviceLock Printer Viewer.

DeviceLock Printer Viewer может отображать данные теневого копирования принтеров в формате PostScript, распечатывать их или сохранять во внешний файл (формата BMP, GIF, JPEG, PNG, EMF или TIFF). Для отображения поддерживаются следующие форматы спулера: PostScript, PCL5, PCL6 (PCL XL), HP-GL/2, GDI printing (ZjStream) и EMF Spooled Files.

Сохранить теневую копию

Нажмите **Сохранить** под нужным результатом поиска. Затем в появившемся диалоговом окне выберите папку и укажите имя файла для хранения копии.

Файлы, отправленные или полученные пользователями, сохраняются в журнале теневого копирования и могут быть сохранены из журнала в локальную или сетевую папку.

Данные, которые пользователи записывают на CD/DVD/BD-диски, сохраняются в журнале теневого копирования в виде образов в формате CUE - один образ на каждый записанный CD/DVD/BD-диск.

Образы CD/DVD/BD-дисков, а также другие данные, которые не были представлены в виде файлов, сохраняются в журнале теневого копирования с именами, созданными автоматически на основе действия пользователя, имени диска или устройства, а также даты/времени (например, `direct_write(E_) 19_18_29 17_07_2006.bin`).

Каждый образ CD/DVD/BD состоит из двух файлов - файла данных `.bin` (например, `direct_write(E_) 19_18_29 17_07_2006.bin`) и файла `.cue` с таким же именем (например, `direct_write(E_) 19_18_29 17_07_2006_bin.cue`). Эти файла позволяют смонтировать CD/DVD/BD-образ в приложениях, поддерживающих формат CUE, таких как Cdrwin, Nero, DAEMON Tools, IsoBuster, UltraISO, WinISO и т.п.

Открыть и сохранить теневую копию во встроенном средстве просмотра

Нажмите **Просмотр** под нужным результатом поиска. Затем в открывшемся окне приложения выберите один из вариантов просмотра:

- **Шестнадцатеричный** - Отображает данные в шестнадцатерично-текстовом режиме.
- **Текст (автоматически)** - Включает автоматический выбор кодировки текста и отображает данные в текстовом режиме.
- **Текст (ANSI)** - Задает кодировку текста ANSI и отображает данные в текстовом режиме.
- **Текст (UTF-16)** - Задает кодировку текста UTF-16 и отображает данные в текстовом режиме.
- **Текст (UTF-16BE)** - Задает кодировку текста UTF-16 с обратным порядком байтов и отображает данные в текстовом режиме.

Чтобы сохранить копию файла, нажмите кнопку **Сохранить**. Затем в появившемся диалоговом окне выберите папку и укажите имя файла для хранения копии.

Автоматизация поиска

Поисковый сервер позволяет сохранять поисковые запросы в виде задач и затем запускать их по расписанию или вручную. При исполнении поисковой задачи сервер сохраняет результаты поиска в отчете, который можно увидеть в консоли. Сервер может автоматически отправлять отчеты с результатами поиска на адреса электронной почты по выбору (для этого требуется почтовый сервер, как описано в разделе Почтовый сервер для отчетов поискового сервера).

Исполняя поисковую задачу, сервер совершает следующие действия:

1. Поиск на основе параметров поискового запроса.
2. Создание и сохранение отчета об исполнении задачи, включая результаты поиска.
3. Отправка отчета по электронной почте, если в задаче указан список получателей.

Поисковые задачи и их отчеты отображаются в дереве консоли под узлом **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи**.

Действия по управлению автоматизацией поиска кратко описываются в следующей таблице. В последующих разделах приводится более подробное описание каждого из этих действий.

Действие	Описание
Создание задачи	Для создания поисковой задачи: • Раскройте **DeviceLock Content Security Server** > **Поисковый сервер** в дереве консоли, щелкните **Задачи** правой кнопкой мыши, щелкните **Создать задачу**, и затем задайте параметры задачи в появившихся диалоговых окнах. Подробнее см. в разделе Создание и настройка новой поисковой задачи.
Просмотр списка задач	Для просмотра списка поисковых задач: • Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** в дереве консоли. Подробнее см. в разделе Управление имеющимися поисковыми задачами.
Управление задачей	Для управления определенной поисковой задачей: • В списке задач, щелкните задачу правой кнопкой мыши, и затем выберите команду в контекстном меню. Подробнее см. в разделе Управление имеющимися поисковыми задачами.
Просмотр списка отчетов	Для просмотра списка отчетов определенной поисковой задачи: • В дереве консоли, раскройте узлы **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи**, и затем выберите задачу под узлом **Задачи**. Подробнее см. в разделе Управление поисковой задачей и ее отчетами.
Управление отчетами	Для управления отчетом определенной поисковой задачи: • В списке отчетов этой задачи, щелкните отчет правой кнопкой мыши, и затем выберите команду в контекстном меню. Подробнее см. в разделе Управление поисковой задачей и ее отчетами.
Просмотр отчета	Для просмотра отчета определенной поисковой задачи: • Выберите отчет в дереве консоли под узлом поисковой задачи. Можно также воспользоваться командой **Открыть** из контекстного меню отчета. Подробнее см. в разделе Просмотр отчета поисковой задачи.

Действие	Описание
Просмотр журнала задач	В журнале задач хранятся сведения о таких событиях как создание, изменение и удаление задач, начало и завершение поиска (включая количество результатов поиска), а также ошибки, произошедшие при настройке или исполнении задач. Для просмотра журнала: • Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли. Подробнее см. в разделе Просмотр и настройка журнала поисковых задач.
Управление журналом задач	Для управления журналом задач: • Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли, щелкните правой кнопкой мыши на панели сведений, и затем выберите команду в контекстном меню. Подробнее см. в разделе Просмотр и настройка журнала поисковых задач.

Создание и настройка новой поисковой задачи

Для создания поисковой задачи требуется выполнить следующие действия:

1. Открыть мастер создания задачи.

   Для этого раскройте узлы **DeviceLock Content Security Server** > **Поисковый сервер** в дереве консоли, щелкните правой кнопкой мыши узел **Задачи** под узлом **Поисковый сервер**, и затем нажмите **Создать задачу**. Для запуска мастера можно также выбрать узел **Задачи** и затем нажать кнопку создания задачи на панели инструментов консоли.

2. Настроить поисковый запрос на первой странице мастера. Подробнее см. в разделе Настройка поискового запроса.

   Настройка поискового запроса аналогична настройке операции полнотекстового поиска (см. Выполнение поиска).

3. При необходимости на второй странице мастера можно изменить имя задачи, настроить расписание запуска задачи, и указать адреса электронной почты получателей отчета. Подробнее см. в разделе Настройка параметров расписания и результатов поиска.

Настройка поискового запроса

На первой странице мастера настройки задач можно задать, просмотреть или изменить параметры, определяющие, какие именно записи журналов и объекты данных будет искать данная задача:

- **Запрос** - Текст поискового запроса. Представляет собой одну или несколько строк, определяющих слова или фразы для поиска. Строки в запросе объединяются по И, так что поиск возвращает результаты, соответствующие каждой из указанных строк.

  В поле **Запрос** можно добавлять группы поиска и сохраненные запросы:

  - Для добавления групп поиска нажмите кнопку **База данных контента**. Затем, в появившемся диалоговом окне выберите требуемые группы и нажмите кнопку **Добавить** или дважды щелкните требуемую группу. Подробнее о группах поиска см. в разделе Управление контентно-зависимыми группами поиска.

    В поле **Запрос** группа поиска представлена ее именем, заключенным в знаки процента: `%имя_группы%`. Группу поиска можно добавить, введя в это поле знак процента и имя группы. По мере ввода в поле **Запрос** появляется список групп, имена которых соответствуют введенному имени. Группу можно выбрать из этого списка.

  - Для добавления ранее сохраненного запроса нажмите кнопку **Сохраненный запрос**. Затем в появившемся диалоговом окне дважды щелкните требуемый запрос или выберите его и нажмите **OK**. Подробнее о сохраненных запросах см. в разделе Управление сохраненными запросами.

  При составлении строки запроса можно использовать команды контекстного меню, появляющегося при щелчке правой кнопкой мыши в поле **Запрос**:

  - **Вставить текст** - Отобразить команды для добавления логических операторов в строку запроса. Оператор `AND`, `OR` и т.п. можно ввести с клавиатуры в верхнем регистре или выбрать из меню **Вставить текст**. Подробнее см. в разделе Обзор логических операторов.

    Чтобы отобразить эти команды, можно также щелкнуть в поле **Запрос** и затем нажать Ctrl+D.

  - **Сохранить как** - Сохранить текущие строки запроса для дальнейшего повторного использования. Подробнее см. в разделе Управление сохраненными запросами.

  Контекстное меню поля **Запрос** содержит также стандартные команды для работы с текстом, такие как **Вырезать**, **Копировать**, **Вставить** и т.п.

- **Показывать** <число> **результатов на странице** - Количество результатов для показа на одной странице отчета.

- **Результаты только из следующих журналов** - Журналы, в которых требуется выполнить поиск. Можно выбрать любую комбинацию следующих журналов:

  - Журнал аудита (выбран по умолчанию)
  - Журнал теневого копирования (выбран по умолчанию)
  - Журнал удаленных данных теневого копирования (выбран по умолчанию)
  - Журнал активности пользователей
  - Журнал сервера
  - Журнал мониторинга
  - Журнал политик

- **Ограничить результаты следующим диапазоном дат** - Ограничение временного промежутка для поиска записей в журналах:
  - **С** - В качестве начала промежутка можно выбрать дату самой ранней записи в журнале (опция **Первой записи**) или указать другую дату (опция **Записи от**). Поиск ведется по записям, выполненным не ранее указанной даты.
  - **По** - В качестве конца промежутка можно выбрать дату самой поздней записи в журнале (опция **Последнюю запись**) или указать другую дату (опция **Записи от**). Поиск ведется по записям, выполненным не позднее указанной даты.
  - **Последние** - Если вместо параметра **С** выбран параметр **Последние**, можно задать поиск по записям в журналах за определенное число дней, недель или месяцев до текущей даты. Необходимо указать желаемое число дней, недель или месяцев.
- **Результаты, удовлетворяющие условиям** - Фильтрация результатов поиска по следующим параметрам:
  - **Отправители** - Можно указать идентификаторы отправителей для следующих протоколов: IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMTP, Telegram, Viber, Web-почта, WhatsApp, Zoom. Поиск возвращает записи, связанные с указанными отправителями.

    Чтобы указать несколько отправителей, используйте точку с запятой (;) в качестве разделителя. Можно использовать знаки подстановки, такие как звездочка (*) и знак вопроса (?).
  - **Получатели** - Можно указать идентификаторы получателей для протоколов IBM Notes, ICQ Messenger, IRC, Jabber, Mail.ru Агент, MAPI, Skype, SMTP, Telegram, Viber, Web-почта, WhatsApp, Zoom, а также следующих социальных сетей: Facebook, Google+, LiveJournal, LinkedIn, LiveInternet, Myspace, Odnoklassniki, Twitter, VKontakte. Поиск возвращает записи, связанные с указанными получателями.

    Чтобы указать несколько получателей, используйте точку с запятой (;) в качестве разделителя. Можно использовать знаки подстановки, такие как звездочка (*) и знак вопроса (?).
  - **Типы файлов** - Можно указать полное или частичное описание типов искомых файлов, например: `E-Mail message (Var.2)`, `Disk Image (Macintosh)`, `Zip 1.0`. Поиск возвращает записи, связанные с любым из указанных файловых типов.

    Чтобы указать несколько типов, используйте точку с запятой (;) в качестве разделителя. Можно использовать знаки подстановки, такие как звездочка (*) и знак вопроса (?).
  - **Источники** - Из выпадающего списка можно выбрать искомые типы устройств или протоколы. Поиск возвращает записи, связанные с любым из выбранных устройств или протоколов.
- **Показывать только новые результаты** - Если этот флажок не установлен, задача возвращает все результаты поиска. Установите этот флажок для того, чтобы исключить результаты предыдущих поисков из результатов текущего поиска. Если этот флажок установлен, задача будет строить отчеты следующим образом:
  - Первый отчет после создания задачи (или после изменения любых параметров поискового запроса задачи) содержит все результаты поиска.
  - Каждый последующий отчет содержит только те результаты поиска, которые не были включены ни в один из предыдущих отчетов.

Внимание: Если в существующей задаче изменить поисковый запрос или любые вышеперечисленные параметры поискового запроса, то первый отчет после таких изменений содержит все результаты поиска, независимо от флажка **Показывать только новые результаты**.

Настройка параметров расписания и результатов поиска

На второй странице мастера настройки задач можно задать, просмотреть или изменить параметры, определяющие как часто сервер будет запускать задачу, как много результатов поиска будет представлено в ее отчетах, и будет ли сервер отправлять результаты поиска по электронной почте. На этой странице мастера предоставляются следующие параметры:

- **Имя задачи** - Имя не может быть пустым или состоять только из пробелов. Каждая задача должна иметь уникальное имя на сервере.
- **Активно** - Если этот флажок установлен, то поисковый сервер будет выполнять задачу по расписанию.
- **Расписание** - Настраиваемое расписание запуска задачи. Можно настроить однократный, ежечасный, ежедневный, еженедельный или ежемесячный запуск задачи:
  - **Однократно** - Однократный запуск. Необходимо указать дату и время запуска задачи, либо установить флажок **Запустить сейчас** для запуска задачи сразу после ее создания или изменения.
  - **Ежечасно** - Ежечасный запуск. Помимо даты и времени необходимо указать интервал запуска задачи. Значение 1 запускает задачу каждый час, а значение 2 - через час.
  - **Ежедневно** - Ежедневный запуск. Помимо даты и времени необходимо указать интервал запуска задачи. Значение 1 запускает задачу каждый день, а значение 2 - через день. Запуск задачи осуществляется ежедневно в соответствии с указанным временем.
  - **Еженедельно** - Еженедельный запуск. Помимо даты и времени необходимо указать интервал запуска задачи и дни недели, по которым задача будет запускаться. Значение 1 запускает задачу каждую неделю, а значение 2 - через неделю. Запуск задачи осуществляется в соответствии с указанным временем в каждый из указанных дней недели.
  - **Ежемесячно** - Ежемесячный запуск. Необходимо указать месяцы, недели месяца и дни недели для каждого месяца, по которым будет выполняться задача. Можно также настроить запуск задачи в определенный последний день недели каждого месяца.
- **Результаты** - Максимальное количество результатов в отчете и адреса для доставки отчета по электронной почте:
  - **Ограничить до** <число> **результатов** - Ограничение числа результатов поиска. Если этот флажок не установлен, большое количество результатов поиска может вызвать перегрузку сервера.
  - **Отправить результаты по e-mail** - Для отправки отчетов с результатами выполнения задачи по электронной почте установите этот флажок и укажите список электронных адресов получателей отчетов. Для разделения адресов в списке используйте точку с запятой (;).

    Для этого параметра требуется заданный почтовый сервер (см. Почтовый сервер для отчетов поискового сервера). Если почтовый сервер в настройках поискового сервера не указан, данный параметр недоступен.
  - **Не отправлять результаты, если ничего не найдено** - Если этот флажок установлен, отправке по электронной почте подлежат только отчеты, содержащие результаты поиска. Пустые отчеты в этом случае не отправляются.

Управление имеющимися поисковыми задачами

Панель сведений отображает список хранящихся на сервере поисковых задач, если в дереве консоли выбрать узел **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи**. По каждой такой задаче в списке предоставляются следующие сведения:

- **Имя** - Имя задачи.
- **Статус** - Одно из следующих значений:
  - **Ожидает** - Запуск задачи по расписанию отключен, задачу можно запустить вручную.
  - **По расписанию** - Запуск задачи по расписанию включен.
  - **Выполняется** - Задача исполняется в данный момент.
  - **Закончена** - Последнее исполнение задачи завершено успешно.
  - **Ошибка** - Последнее исполнение задачи завершилось с ошибкой.
- **Расписание** - Расписание запуска задачи.
- **Найдено результатов** - Общее количество результатов поиска по всем запускам задачи. В скобках указывается количество результатов поиска для последнего запуска задачи.
- **Отправлять результаты** - Адреса электронной почты для рассылки отчетов по данной задаче. Пусто, если отправка отчетов по электронной почте не настроена в параметрах задачи.
- **Время последнего запуска** - Дата и время последнего запуска данной задачи.

Контекстное меню узла **Задачи** содержит следующие команды:

- **Создать задачу** - Создать новую задачу. Параметры задачи можно задать в диалоговых окнах, которые открывает эта команда. Подробнее см. в разделе Создание и настройка новой поисковой задачи.
- **Сохранить все задачи** - Экспортировать все задачи в файл.
- **Загрузить задачи** - Импортировать поисковые задачи из файла.

  Задачи можно экспортировать в файл и затем импортировать их из этого файла. Эта возможность может быть полезной, например, при необходимости скопировать задачи на другой сервер. Подробнее см. в разделе Экспорт и импорт задач.
- **Обновить** - Обновить список задач с учетом последних изменений.

Контекстное меню поисковой задачи на панели сведений содержит следующие команды:

- **Редактировать задачу** - Просмотреть или изменить параметры задачи можно в диалоговых окнах, которые открывает эта команда.
- **Дублировать задачу** - Создать новую задачу путем копирования параметров выбранной задачи. Параметры новой задачи можно редактировать в диалоговых окнах, которые открывает эта команда.

  Имя новой задачи по умолчанию состоит из префикса “Копия”, за которым следует имя выбранной задачи. При создании двух или более копий к новому имени по умолчанию добавляется числовой суффикс, указывающий номер копии.
- **Удалить задачу** - Удалить выбранную задачу.

  Если данная задача уже запускалась и имеет отчеты, то удалить ее невозможно. Для удаления такой задачи требуется сначала удалить все ее отчеты.
- **Экспортировать задачу** - Экспортировать задачу в файл.

  Восстановить задачу из файла можно с помощью команды **Загрузить задачи** на узле **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** в дереве консоли.

- **Запустить задачу** - Немедленный запуск задачи независимо от расписания.
- **Остановить задачу** - Немедленно прекратить исполнение выбранной задачи. Эта команда появляется вместо команды **Запустить задачу** для задач, которые в данный момент исполняются.
- **Обновить** - Обновить список задач с учетом последних изменений.

Команды контекстного меню можно использовать для выполнения следующих действий:

- **Запустить данную задачу** - Щелкните задачу правой кнопкой мыши и затем выберите команду **Запустить задачу**.
- **Просмотреть или изменить поисковый запрос данной задачи** - Щелкните задачу правой кнопкой мыши, выберите команду **Редактировать задачу** и затем выполните шаги по настройке поискового запроса, описанные выше в разделе Создание и настройка новой поисковой задачи.
- **Просмотреть или изменить имя, расписание или параметры результатов данной задачи** - Щелкните задачу правой кнопкой мыши, выберите команду **Редактировать задачу**, и затем выполните шаги по настройке имени, а также параметров расписания и результатов, описанные выше в разделе Создание и настройка новой поисковой задачи.

  В мастере редактирования задачи используются те же страницы, что и в мастере создания задачи. Единственное отличие в том, что страницы мастера редактирования отображают текущие значения параметров задачи и позволяют вносить изменения в выбранную задачу, без создания новой.
- **Создать новую задачу путем копирования параметров данной задачи** - Щелкните правой кнопкой мыши задачу для копирования, выберите команду **Дублировать задачу** и затем выполните шаги по созданию новой задачи, описанные выше в разделе Создание и настройка новой поисковой задачи.

  В мастере копирования задачи используются те же страницы, что и в мастере создания задачи. Единственное отличие в том, что страницы мастера копирования уже заполнены значениями параметров, скопированными из выбранной задачи.
- **Удалить данную задачу** - Допускается удаление только задач, не содержащих ни одного отчета. Дважды щелкните задачу, чтобы увидеть список ее отчетов. Затем, нажмите Ctrl+A для выбора всех отчетов в списке, щелкните правой кнопкой мыши на выбранных отчетах и выберите команду **Удалить отчеты**. После удаления всех отчетов, вернитесь к списку задач, щелкнув узел **Задачи** в дереве консоли, щелкните задачу правой кнопкой мыши, и затем выберите команду **Удалить**.

Экспорт и импорт задач

Задачи можно экспортировать в файл и затем импортировать их из этого файла. Эта возможность может быть полезной, например, при необходимости скопировать задачи на другой сервер. Возможен как экспорт отдельной задачи, так и экспорт всех задач сразу.

Чтобы экспортировать задачу

1. В дереве консоли, выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи**.
2. На панели сведений, щелкните задачу правой кнопкой мыши, выберите команду **Экспортировать задачу** и затем укажите файл для хранения экспортированной задачи.

Чтобы экспортировать все задачи

1. В дереве консоли, выберите **DeviceLock Content Security Server** > **Поисковый сервер**.
2. На панели сведений, щелкните **Задачи** правой кнопкой мыши, выберите команду **Сохранить все задачи** и затем укажите файл для хранения экспортированных задач.

Чтобы импортировать задачи из файла

1. В дереве консоли, выберите **DeviceLock Content Security Server** > **Поисковый сервер**.
2. На панели сведений, щелкните **Задачи** правой кнопкой мыши, выберите команду **Загрузить задачи** и затем укажите файл, в котором хранятся ранее экспортированные задачи.

Управление поисковой задачей и ее отчетами

Поисковые задачи отображаются в дереве консоли под узлом **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи**. Контекстное меню задачи в дереве консоли содержит те же команды, что и меню задачи в области сведений (см. Управление имеющимися поисковыми задачами).

Выбрав поисковую задачу в дереве консоли, можно увидеть список всех отчетов, созданных этой задачей. Панель сведений отображает список отчетов со следующими сведениями по каждому отчету:

- **Имя** - Имя отчета содержит имя задачи, а также дату и время запуска задачи.
- **Тип** - Возможные значения: **По расписанию** (задача была запущена по расписанию) или **Вручную** (задача была запущена вручную).
- **Статус** - Возможные значения:
  - **Создание** - Создание отчета продолжается.
  - **Готово** - Отчет создан успешно.
  - **Ошибка** - Отчет завершился с ошибкой.
- **Найдено результатов** - Количество результатов поиска в отчете.
- **Отправлен** - Возможные значения:
  - **Да** - Отчет успешно отправлен по электронной почте хотя бы одному получателю.
  - **Нет** - Не указано ни одного получателя этого отчета по электронной почте или не удалось доставить отчет никому из получателей.
- **Запущен** - Дата и время начала создания отчета.
- **Закончен** - Дата и время завершения создания отчета.
- **Запущено** - Учетная запись, запустившая задачу поиска.
- **С компьютера** - Компьютер, с которого задача поиска была запущена.

Для управления отчетом можно щелкнуть отчет правой кнопкой мыши и использовать следующие команды из появившегося контекстного меню:

- **Открыть** - Отобразить отчет на панели сведений.

  Отобразить отчет можно также выбрав его под узлом задачи в дереве консоли.
- **Отправить отчет по e-mail** - Отправить отчет по электронной почте. Адресаты указываются после выбора этой команды.

  Эта команда доступна, только если отчет имеет статус **Готово** и задан почтовый сервер (см. Почтовый сервер для отчетов поискового сервера).
- **Переименовать** - Изменить имя отчета.
- **Удалить отчет** - Удалить выбранный отчет.

  Для удаления сразу нескольких отчетов выбирайте отчеты щелчком мыши, удерживая нажатой клавишу Shift или Ctrl; затем щелкните правой кнопкой мыши выбранные отчеты и выберите команду **Удалить отчеты**.
- **Обновить** - Обновляет список отчетов с учетом последних изменений.

Список отчетов поисковой задачи отображается также в дереве консоли, под узлом, представляющим эту задачу. Например, для задачи с именем **Офис** дерево консоли отображает список отчетов под узлом **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Офис**. Панель сведений отображает тот же список отчетов при выборе узла **Офис** в дереве консоли.

Чтобы открыть отчет, выполните любое из следующих действий:

- Выберите отчет в дереве консоли.
- Дважды щелкните отчет на панели сведений.

Просмотр отчета поисковой задачи

Раскрыв узел поисковой задачи, в дереве консоли можно выбрать любой из отчетов этой задачи. При выборе отчета в дереве консоли, панель сведений отображает страницы отчета, аналогичные страницам узла **Страница поиска**. Отобразить отчет можно также командой **Открыть** из контекстного меню или двойным щелчком в списке отчетов на панели сведений консоли. Контекстное меню отчета в дереве консоли содержит те же команды, что и меню отчета в области сведений (см. Управление поисковой задачей и ее отчетами).

Каждая страница отчета содержит заголовок отчета и список результатов поиска.

Заголовок отчета отображает имя и идентификационный номер отчета, а также содержит следующую информацию об отчете:

- **Запущен** - Дата и время начала создания отчета.
- **Закончен** - Дата и время завершения создания отчета.
- **Пользователь** - Учетная запись, от имени которой задача поиска была запущена.
- **Компьютер** - Компьютер, с которого задача поиска была запущена.
- **Найдено результатов** - Количество результатов, найденных задачей поиска.
- **Включено в отчет** - Количество результатов поиска, включенных в отчет.

  Значение **Включено в отчет** может отличаться от значения **Найдено результатов**, если параметры задачи ограничивают число результатов поиска в отчете, или поиск вернул более 100,000 результатов.
- **Настройки поиска** - Нажмите кнопку **Настройки поиска** для просмотра параметров поискового запроса, выполненного задачей поиска.

  Область **Настройки поиска** отображает только настроенные параметры, с теми же именами, что в мастере создания поисковой задачи. Параметры, значения которых не заданы, в заголовке отчета не отображаются.

Список результатов поиска имеет тот же вид и те же функции, что и список результатов поиска, отображаемый на страницах узла **Страница поиска**:

- Строка статистики - Показывает количество результатов поиска, отображённых на текущей странице отчета.
- Область результатов поиска - Показывает нумерованный список найденных результатов, соответствующих заданным критериям поиска. Подробнее о списке результатов поиска см. в разделе Область результатов поиска.
- Навигатор результатов - Показывает количество страниц отчета и позволяет переходить с одной страницы на другую.

Отчеты, доставляемые по электронной почте, выглядят так же, как в консоли. Единственное их отличие от "консольных" отчетов состоит в том, что "почтовые" отчеты не разбиты на страницы и не предоставляют интерактивный доступ к данным теневого копирования из списка результатов поиска.

Консоль скрывает результаты поиска, относящиеся к журналу теневого копирования, если пользователь консоли не является администратором сервера DeviceLock Content Security Server с правом доступа к данным теневого копирования. Для пользователей, которые не обладают этим правом, консоль заменяет такие результаты поиска звездочками. В "почтовых" отчетах результаты поиска по журналу теневого копирования заменяются звездочками, если пользователь, запрашивающий отправку отчета по электронной почте, не имеет права доступа к данным теневого копирования. Для раскрытия данных теневого копирования в "почтовом" отчете требуются следующие условия:

- Если отправка отчета выполняется поисковой задачей, пользователь, запускающий ее при помощи команды **Запустить задачу** в консоли, должен обладать правом доступа к данным теневого копирования.
- Пользователь, отправляющий отчет при помощи команды **Отправить отчет по e-mail** в консоли, должен обладать правом доступа к данным теневого копирования.

Просмотр и настройка журнала поисковых задач

В журнале задач протоколируются такие события как создание, изменение и удаление задач, начало и завершение поиска, данные о количестве найденных объектов, а также ошибки, имевшие место при настройке или исполнении поисковых задач.

Консоль отображает список событий при выборе узла **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли, предоставляя следующую информацию по каждому событию:

- **Тип** - Тип события. Возможные значения:
  - **Успех** - Задача или операция завершена успешно.
  - **Информация** - Выполнено определенное действие.
  - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
  - **Ошибка** - Возникла ошибка.
- **Дата/Время** - Дата и время события.
- **Событие** - Идентификационный номер события.
- **Имя задачи** - Имя поисковой задачи, вызвавшей событие.
- **Информация** - Описание события, включая описание действий и ошибок.
- **Сервер** - Имя компьютера, на котором произошло событие.
- **Запись N** - Порядковый номер записи в списке событий.

Для управления журналом задач можно щелкнуть правой кнопкой мыши в списке событий и использовать следующие команды из появившегося контекстного меню:

- **Настройки** - Просмотреть или изменить параметры, ограничивающие максимальное число записей в журнале. См. также Управление настройками журнала.
- **Сохранить** - Сохранить журнал в указанный файл.
- **Обновить** - Обновить список событий с учетом последних изменений.
- **Фильтр** - Задать условия фильтрации списка событий. См. также Фильтрация журнала.
- **Быстрые фильтры** - Применить быструю фильтрацию списка событий в одном из следующих вариантов:
  - **Текущий день** - Показать события только за текущий день.
  - **Текущая неделя** - Показать события только за текущую неделю.
  - **Текущий месяц** - Показать события только за текущий месяц.
  - **Текущий год** - Показать события только за текущий год.

  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).
- **Удалить фильтр** - Показать все записи, отключив примененный фильтр.
- **Очистить** - Удалить все записи из журнала, одновременно добавляя запись об очистке журнала с указанием числа удаленных записей.

Управление настройками журнала

Для просмотра или изменения настроек журнала поисковых задач выполните следующие действия:

1. Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли, щелкните правой кнопкой мыши на панели сведений и затем выберите команду **Настройки**.
2. В появившемся диалоговом окне можно просмотреть или изменить следующие параметры:
   - **Контролировать размер журнала** - Установите этот флажок, чтобы разрешить серверу контролировать количество записей в журнале и удалять устаревшие записи. Если этот флажок не установлен, сервер использует все доступное пространство базы данных для хранения журнала.
   - **Сохранять события за последние** <число> **дней** - Выберите этот параметр, чтобы хранить записи не старше определенного количества дней. Затем задайте нужное количество дней. Значение по умолчанию - 365 дней.
   - **Максимальный размер:** <число> **записей** - Выберите этот параметр, чтобы хранить не более определенного количества записей. Затем укажите нужное количество записей и выберите действие сервера, которое будет выполняться, когда журнал достигнет максимального размера:
     - **Затирать старые события по необходимости** - Новые записи событий продолжают сохраняться при достижении максимального размера журнала. Каждая запись нового события заменяет собой самую старую запись в журнале.
     - **Затирать события старше** <число> **дней** - Новые записи событий заменяют собой только записи, хранящиеся дольше заданного количества дней. Поддерживаемая настройка - до 32 767 дней.
     - **Не затирать события (очистка журнала вручную)** - При достижении максимального размера журнала новые записи событий не добавляются. Чтобы обеспечить их добавление, необходимо очистить журнал вручную.

   Внимание: Если в журнале нет места для новых записей, а настройки журнала не позволяют удалить старые записи, сервер не будет добавлять новые записи в журнал.

   Чтобы использовать размер журнала по умолчанию, выберите параметр **Максимальный размер** и нажмите кнопку **Восстановить умолчания**. В результате будут установлены следующие настройки:
   - Максимальный размер: 10 000 записей
   - Затирать события старше 7 дней
3. Для сохранения изменений нажмите кнопку **OK**.

Фильтрация журнала

Чтобы настроить фильтр для журнала поисковых задач, выполните следующие действия:

1. Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли, щелкните правой кнопкой мыши на панели сведений и затем выберите команду **Фильтр**.
2. В появившемся диалоговом окне, можно настроить следующие параметры фильтрации:
   - **Включить** - Отображать в списке только события, удовлетворяющие условиям, заданным на вкладке **Включить**. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Включить**.
   - **Исключить** - Не отображать в списке события, удовлетворяющие условиям, заданным на вкладке **Исключить**. Чтобы настроить и применить эти условия, установите флажок **Включить фильтр** на вкладке **Исключить**.

     Примечание: Значок рядом с именем вкладки становится зеленым, если фильтр на данной вкладке включен. В противном случае цвет этого значка серый.

   - **Типы событий** - Фильтрация по типу событий. Возможны следующие варианты (установите соответствующие флажки):
     - **Успех** - Задача или операция завершена успешно.
     - **Информация** - Выполнено определенное действие.
     - **Предупреждение** - Возможны осложнения или ошибки, если не предпринять никаких действий.
     - **Ошибка** - Произошла ошибка.
   - **Имя задачи**, **Информация**, **Сервер**, **ID-события** - Включение или исключение из списка событий, у которых в указанном поле данных встречается заданная строка.

     Например, для фильтрации событий по имени задачи, укажите строку фильтра в поле **Имя задачи**. Для фильтрации событий с определенными номерами, напечатайте номера искомых событий в поле **ID-события**, используя точку с запятой в качестве разделителя.

     Примечание: Чтобы облегчить настройку фильтра, строковые поля запоминают ранее вводившиеся данные и подставляют подходящие строки по мере ввода с клавиатуры. История введенных значений доступна в раскрывающемся списке параметров поля.

   - **С** - Определяет начало временного интервала событий для фильтрации. Возможные значения: **Первой записи** (значение по умолчанию) и **Записи от**. Выберите **Первой записи**, чтобы фильтровать события, начиная с самого раннего в журнале. Выберите **Записи от**, чтобы фильтровать события, произошедшие не ранее определенной даты и времени.
   - **По** - Определяет конец временного интервала событий для фильтрации. Возможные значения: **Последнюю запись** (значение по умолчанию) и **Записи от**. Выберите **Последнюю запись**, чтобы фильтровать события, заканчивая самым поздним в журнале. Выберите **Записи от**, чтобы фильтровать события, произошедшие не позднее определенной даты и времени.
3. Для сохранения изменений нажмите кнопку **OK**.

Настраивая фильтр, учитывайте следующее:

- Условия фильтра объединяются по И, так что запись соответствует фильтру, если она соответствует каждому условию фильтра. Оставляйте пустыми поля, которые не должны использоваться в условиях фильтра.
- В строковых полях фильтра допускаются знаки подстановки, такие как звездочка и вопросительный знак. Звездочка (*) обозначает любую (в том числе пустую) группу символов. Вопросительный знак (?) обозначает любой одиночный символ.
- В любом строковом поле фильтра можно указать несколько значений, разделяя их точкой с запятой (;). Значения в этом случае объединяются по ИЛИ, так что запись соответствует условию фильтра по данному полю, если она соответствует хотя бы одному из указанных в этом поле значений.
- Кнопка **Очистить** в диалоговом окне **Фильтр** позволяет удалить все ранее заданные условия и начать настройку нового фильтра с нуля.
- Кнопки **Сохранить** и **Загрузить** в диалоговом окне **Фильтр** служат для сохранения условий фильтра в файл и загрузки ранее сохраненных условий из файла.

Сузить список событий можно также при помощи быстрой фильтрации:

- Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли, щелкните правой кнопкой мыши на панели сведений, укажите на **Быстрые фильтры** и затем выберите один из вариантов быстрого фильтра:
  - **Текущий день** - Показать события только за текущий день.
  - **Текущая неделя** - Показать события только за текущую неделю.
  - **Текущий месяц** - Показать события только за текущий месяц.
  - **Текущий год** - Показать события только за текущий год.

  Для отмены примененного быстрого фильтра выберите тот же вариант фильтра еще раз или используйте команду **Удалить фильтр**.

  Обычный фильтр, включенный командой **Фильтр**, делает невозможным применение быстрых фильтров и отменяет имеющийся быстрый фильтр (если он был применен). Чтобы задействовать быстрые фильтры, отключите обычный фильтр (например, при помощи команды **Удалить фильтр**).

Обновление списка событий, сохранение и очистка журнала

При просмотре журнала можно также:

- Обновить список событий с учетом последних данных - Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли, щелкните правой кнопкой мыши на панели сведений и затем выберите команду **Обновить**.
- Сохранить журнал в текстовый файл - Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли, щелкните правой кнопкой мыши на панели сведений, выберите команду **Сохранить** и затем укажите файл для сохранения журнала.
- Удалить все записи из журнала - Выберите **DeviceLock Content Security Server** > **Поисковый сервер** > **Задачи** > **Просмотрщик журнала** в дереве консоли, щелкните правой кнопкой мыши на панели сведений и затем выберите команду **Очистить**.

  После удаления всех записей из журнала, команда **Очистить** записывает в журнал событие с информацией об удалении записей и количестве удаленных записей.

Типы файлов, индексируемых для поиска

Поисковый сервер способен индексировать и выполнять поиск в документах, представленных файлами следующих форматов/типов:

- Adobe Framemaker MIF (*.mif)
- Adobe Photoshop images (только метаданные) (*.psd)
- Ami Pro (*.sam)
- Ansi Text (*.txt)
- Apple iWork KeyNote 2009 (*.key)
- Apple iWork Numbers 2009 (*.numbers)
- Apple iWork Pages 2009 (*.pages)
- ASCII Text
- Медиа-файлы ASF (только метаданные) (*.asf)
- CSV (значения, разделенные запятыми) (*.csv)
- DBF (*.dbf)
- EBCDIC
- EML (почтовые сообщения, сохраненные приложением Outlook Express) (*.eml)
- Enhanced Metafile Format (*.emf)
- EMF Spool (*.spl)
- Файлы сообщений Eudora MBX (*.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?)
- Почтовые архивы MBOX, включая вложения (*.mbx)
- Архивы веб-страниц MHT (*.mht)
- Сообщения в формате MIME, включая вложения
- MSG (почтовые сообщения, сохраненные приложением Outlook), включая вложения (*.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)
- Файлы данных Microsoft Outlook 97, 2000, 2003, 2007, 2010, 2013, 2016, включая вложения (*.PST, *.OST)
- Сообщения, заметки, назначения и задачи Microsoft Outlook/Exchange
- Хранилища сообщений Microsoft Outlook Express 5 и 6 (*.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 (только метаданные) (*.mp3)
- Multimate Advantage II (*.dox)
- Multimate version 4 (*.doc)
- Документы, презентации и электронные таблицы OpenOffice/LibreOffice версий 1, 2, 3, 4, 5 (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf)
- Файлы PDF (*.pdf)

  Примечание: Зашифрованный файл PDF может быть проиндексирован, только если его можно открыть без пароля, и права доступа в нем позволяют извлекать текст.

- Файлы PDF Portfolio (*.pdf), включая вложенные документы в формате, отличном от PDF
- Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw)
- QuickTime (*.mov, *.m4a, *.m4v)
- RAR (*.rar)
- TAR (*.tar)
- TIFF (только метаданные) (*.tif)
- TNEF (winmail.dat)
- Treepad HJT files (*.hjt)
- Unicode (UCS 16, порядок байтов для Mac или Windows, или UTF-8)
- Файлы Visio XML (*.vdx)
- Windows Metafile Format (*.wmf)
- Медиа-файлы WMA (только метаданные) (*.wma)
- Видео-файлы WMV (только метаданные) (*.wmv)
- WordPerfect 4.2 (*.wpd, *.wpf)
- WordPerfect (версии 5.0 и выше) (*.wpd, *.wpf)

- WordStar версий 1, 2, 3, 4, 5, 6 (*.ws)
- WordStar 2000
- Write (*.wri)
- XBase, в том числе FoxPro, dBase и прочие совместимые с XBase форматы (*.dbf)
- XML (*.xml)
- XML Paper Specification (*.xps)
- XSL
- XyWrite
- ZIP (совместимый с PKZIP 2.0) (*.zip)

15

Приложение: Активация лицензий DeviceLock

Данная глава содержит информацию о лицензировании программного комплекса DeviceLock и его дополнительных компонентов с помощью лицензионных файлов DeviceLock.

В этой главе:

О типах лицензий DeviceLock

Активация клиентских лицензий

Активация серверных лицензий

О типах лицензий DeviceLock

Лицензирование DeviceLock основано на количестве контролируемых конечных точек. В лицензии указывается количество таких точек, где можно задавать политики DeviceLock и обеспечивать их соблюдение. Контролируемой конечной точкой может быть:

- Настольный компьютер, ноутбук или сервер
- Виртуальная машина
- Сеанс удаленного рабочего стола / виртуального приложения

В последнем случае каждый сеанс считается отдельной контролируемой точкой. Количество контролируемых конечных точек в лицензии DeviceLock должно соответствовать количеству сеансов, запущенных на сервере виртуализации. Например, при развертывании DeviceLock на сервере удаленного рабочего стола необходимо, чтобы количество контролируемых конечных точек в лицензии DeviceLock соответствовало количеству запущенных на сервере сеансов удаленного рабочего стола.

Поскольку DeviceLock имеет ряд дополнительных компонентов, существует несколько типов лицензий:

Тип лицензии	Имя файла лицензии
Основная (Core)	devicelock.lic
ContentLock	dlcl.lic
NetworkLock	dlnl.lic
Мониторинг активности пользователей (UAM)	dluam.lic
Поисковый сервер (Search Server)	dlss.lic
Сервер обнаружения (Discovery)	dlds.lic

Основная лицензия является обязательной, остальные лицензии относятся к дополнительным компонентам. Чтобы использовать дополнительный компонент, его лицензия должна быть активирована в дополнение к основной лицензии. Без основной лицензии другие лицензии не действуют (кроме лицензии на сервер Discovery).

Если основная лицензия отсутствует, повреждена или истекла, все компоненты DeviceLock (кроме сервера Discovery) работают в пробном режиме. Для сервера Discovery основная лицензия не требуется.

Количество лицензий ContentLock, NetworkLock и/или UAM (мониторинг активности пользователей) должно соответствовать количеству основных лицензий, иначе соответствующие дополнительные компоненты считаются не лицензированными.

Пример

Предположим, что на компьютере, на котором работает консоль DeviceLock Management Console, активировано следующее количество лицензий: основных лицензий (Core) - 1 000; лицензий ContentLock - 1 000; лицензий NetworkLock - 1 000; лицензий UAM - 1 000.

Затем на этом компьютере дополнительно активируют 100 основных лицензий, так что их общее количество превосходит количество лицензий ContentLock, NetworkLock и UAM: основных лицензий - 1 100; лицензий ContentLock - 1 000; лицензий NetworkLock - 1 000; лицензий UAM - 1 000.

В результате компоненты ContentLock, NetworkLock и UAM переходят в пробный режим, так что их дальнейшая настройка и использование становятся невозможными.

Описанную в этом примере проблему можно решить путем активации 100 дополнительных лицензий ContentLock, NetworkLock и UAM на компьютере консоли DeviceLock Management Console, где активировано 1 100 основных лицензий. Еще один вариант решения проблемы - удалить 100 основных лицензий с этого компьютера и активировать их на другом компьютере с с консолью DeviceLock Management Console, где нет лицензий ContentLock, NetworkLock и UAM. Этот экземпляр консоли DeviceLock Management Console сможет управлять 100 компьютерами, но без функций ContentLock, NetworkLock и UAM.

Активация клиентских лицензий

Для использования DeviceLock необходимо активировать основную лицензию (Core license). Чтобы использовать модули ContentLock / NetworkLock и мониторинг пользователей (UAM), необходимо активировать соответствующие лицензии в дополнение к основной лицензии.

Основная лицензия активируется на компьютерах, на которых работает консоль DeviceLock Management Console или сервер DeviceLock Enterprise Server, то есть на тех компьютерах, которые используются для управления сервисом DeviceLock на других компьютерах или для сбора данных с компьютеров, контролируемых сервисом DeviceLock.

Чтобы активировать основную лицензию, скопируйте файл `devicelock.lic` в папку установки DeviceLock и запустите консоль DeviceLock Management Console для его распознавания. Папка установки по умолчанию - `%ProgramFiles%\DeviceLock` или `%ProgramFiles(x86)%\DeviceLock` в 32-разрядной или 64-разрядной системе, соответственно.

Лицензии ContentLock, NetworkLock и UAM активируются на тех же компьютерах, что и основная лицензия. Скопируйте файлы лицензий (например, `dlcl.lic`, `dlnl.lic` и `dluam.lic`) в папку установки DeviceLock, а затем запустите консоль DeviceLock Management Console для их активации.

При запуске DeviceLock Management Console автоматически распознает файлы лицензий, имеющиеся в папке установки DeviceLock, и соответственно активирует лицензии. Никаких дополнительных действий не требуется.

Примечание:

- Изначально имя файлов лицензии DeviceLock имеет расширение `.lic`. Когда лицензия активирована, расширение изменяется на `.li_`.
- В папку установки можно скопировать несколько файлов лицензии, присвоив каждому из них уникальное имя. Например, `devicelock.lic`, `devicelock1.lic`, `dlcl.lic`, `dlcl2.lic` и т.д.

Рекомендации

После замены файла лицензии DeviceLock с истекшим периодом обновлений на действительный может оказаться, что на странице "О программе DeviceLock" в консоли управления по-прежнему отображается информация об устаревшей лицензии. Данная проблема обычно вызвана тем, что устаревший лицензионный файл был заменен действительным лицензионным файлом с тем же именем.

Для устранения проблемы необходимо выполнить следующие действия:

1. Удалите файл лицензии из папки установки DeviceLock. По умолчанию это папка `%ProgramFiles%\DeviceLock` или `%ProgramFiles(x86)%\DeviceLock` в 32-разрядной или 64-разрядной системе, соответственно.
2. Запустите редактор реестра `regedit.exe`. В 32-разрядной системе удалите значение реестра `HKLM\SOFTWARE\SmartLine Vision\LIC`. В 64-разрядной системе удалите значение реестра `HKLM\SOFTWARE\Wow6432Node\SmartLine Vision\LIC`.
3. Скопируйте новый файл лицензии в папку установки DeviceLock и запустите консоль DeviceLock Management Console для его активации.

Активация серверных лицензий

Для поискового сервера и сервера Discovery необходимы дополнительные лицензии. Для сервера DeviceLock Enterprise Server требуется основная лицензия DeviceLock, а также лицензия UAM при необходимости сбора данных мониторинга пользователей (см. Просмотр активности пользователей).

Enterprise Server

Сервер DeviceLock Enterprise Server является необязательным компонентом, не требующим дополнительной лицензии. Уже имеющейся основной лицензии DeviceLock достаточно, чтобы установить столько экземпляров этого сервера, сколько необходимо для распределения нагрузки между ними.

Для сбора журналов сервиса DeviceLock на сервере DeviceLock Enterprise Server должна быть активирована основная лицензия DeviceLock.

Для применения настроек модулей ContentLock и/или NetworkLock с помощью серверных политик и задач мониторинга компьютеров на сервере DeviceLock Enterprise Server должна быть активирована лицензия ContentLock и/или NetworkLock.

Для применения настроек и правил мониторинга пользователей с помощью серверных политик и задач мониторинга компьютеров на сервере DeviceLock Enterprise Server должна быть активирована лицензия DeviceLock UAM.

Для активации лицензии установите ее файл (например, `devicelock.lic` или `dluam.lic`) с помощью консоли DeviceLock Management Console:

1. Подключите консоль к серверу DeviceLock Enterprise Server.
2. В дереве консоли выберите узел **DeviceLock Enterprise Server** > Настройки сервера.
3. Дважды щелкните параметр **Лицензии DeviceLock** на панели сведений и затем загрузите файл лицензии в появившемся диалоговом окне.

Поисковый сервер

Поисковый сервер (входит в состав сервера DeviceLock Content Security Server) используется для индексирования и поиска документов, собранных в журналах DeviceLock Enterprise Server. Чтобы использовать этот сервер, необходимо активировать его лицензию. Кроме того, необходимо активировать основную лицензию на сервере DeviceLock Enterprise Server.

Для активации лицензии установите ее файл (например, `dlss.lic`) с помощью консоли DeviceLock Management Console:

1. Подключите консоль к серверу DeviceLock Content Security Server.
2. В дереве консоли выберите узел **DeviceLock Content Security Server** > Настройки сервера > Настройки поискового сервера.
3. Дважды щелкните параметр **Лицензии поискового сервера** на панели сведений и затем загрузите файл лицензии в появившемся диалоговом окне.

Сервер Discovery

Сервер Discovery (входит в состав сервера DeviceLock Content Security Server) служит для сканирования пользовательских компьютеров и файловых хранилищ с целью обнаружения контента и данных определенного типа в соответствии настраиваемыми правилами. Чтобы использовать этот сервер, необходимо активировать его лицензию. Основная лицензия DeviceLock не требуется.

Для активации лицензии установите ее файл (например, `dlds.lic`) с помощью консоли DeviceLock Management Console:

1. Подключите консоль к серверу DeviceLock Content Security Server.
2. В дереве консоли выберите узел **DeviceLock Content Security Server** > **Настройки сервера** > **Настройки сервера Discovery**.
3. Дважды щелкните параметр **Лицензии Discovery Server** на панели сведений и затем загрузите файл лицензии в появившемся диалоговом окне.

16

Приложение: Консолидация журналов в облаке с помощью OpenVPN

В этой главе:

Обзор требований

Настройка облачного сервера

Настройка локальных серверов

Обзор требований

При консолидации журналов DeviceLock (см. Консолидация журналов) внутри локальной сети серверы обмениваются данными при помощи удаленного вызова процедур (RPC) по протоколу TCP/IP. Этот метод обеспечивает быструю и эффективную связь в корпоративной сети.

Связь с облачным сервером через RPC может быть обеспечена через защищенное соединение виртуальной частной сети (VPN) с использованием программного обеспечения OpenVPN. Здесь приводится инструкция по настройке сервера и клиента OpenVPN, а также сервера DeviceLock Enterprise Server для консолидации журналов DeviceLock на облачном сервере.

Для консолидации журналов DeviceLock с назначенных локальных серверов на облачный сервер через VPN-соединение с использованием OpenVPN необходимы следующие условия:

- Локальные серверы могут получить доступ к облачному компьютеру по его IP-адресу.

  Это требование выполняется, например, когда локальный компьютер имеет доступ к интернету, а облачный компьютер имеет статический общедоступный IP-адрес и, таким образом, напрямую доступен через интернет.

- На локальном и на облачном компьютере брандмауэр Windows настроен так, что:
  - Порт 80 открыт для входящего публичного TCP-трафика.
  - Серверу DeviceLock Enterprise Server разрешен входящий публичный TCP-трафик.

  Чтобы выполнить эти требования, с помощью консоли “Монитор брандмауэра Защитника Windows в режиме повышенной безопасности” (`wf.msc`) создайте правила для входящих подключений со следующими параметрами:

  - Тип правила - `Для порта`; Локальный порт - `80`;
    Действие - `Разрешить подключение`; Профиль - `Публичный`.
  - Тип правила - `Для программы`; Путь программы - `%ProgramFiles%(x86)\DeviceLock\DLServer.exe`;
    Действие - `Разрешить подключение`; Профиль - `Публичный`.

- На облачном компьютере установлен и настроен сервер OpenVPN.
- На локальном компьютере установлен и настроен клиент OpenVPN.

- Серверу DeviceLock Enterprise Server на облачном и локальном компьютере назначен фиксированный сетевой порт. Обычно это порт `9133`.
- Локальный сервер DeviceLock Enterprise Server использует сертификат DeviceLock для аутентификации на облачном сервере DeviceLock Enterprise Server.

В данной инструкции предполагается, что DeviceLock Enterprise Server установлен, запущен и работает на облачном и на локальном компьютере. Наша цель - сделать локальный DeviceLock Enterprise Server удаленным сервером консолидации для работающего в облаке сервера DeviceLock Enterprise Server. В результате облачный сервер будет консолидировать журналы с локального сервера. Таким же образом можно настроить консолидацию журналов с нескольких локальных серверов.

Кроме того, описанная ниже настройка позволит консоли DeviceLock Management Console с локального компьютера подключаться и управлять облачным сервером DeviceLock Enterprise Server.

Настройка облачного сервера

На облачном компьютере необходимо установить и настроить сервер OpenVPN, и подготовить сервер DeviceLock Enterprise Server к обслуживанию запросов на консолидацию с локальных серверов.

В этом разделе рассматриваются следующие задачи по настройке облачного сервера:

- Установить OpenVPN
- Подготовить сертификаты сервера
- Настроить сервер OpenVPN
- Настроить DeviceLock Enterprise Server

Установить OpenVPN

Загрузите исполняемый файл установки OpenVPN для Windows с сайта openvpn.net/community-downloads (файл .exe). Запустите этот файл и следуйте инструкциям мастера установки:

- Установите все компоненты, в том числе **EasyRSA 2 Certificate Management Scripts**. Этот компонент понадобится для создания сертификатов.
- Примите папку установки по умолчанию, `%ProgramFiles%\OpenVPN`. В этой папке будет также храниться конфигурация сервера OpenVPN.
- При появлении запроса согласитесь установить программное обеспечение устройства TAP. Это виртуальное сетевое устройство обеспечивает соединение и обмен данными между сервером OpenVPN и его клиентами.
- Для OpenVPN требуется Microsoft .NET Framework 4.0 или более поздней версии. По запросу мастера установите последнюю версию .NET Framework. Инструкции по установке см. в статье Microsoft по адресу docs.microsoft.com/dotnet/framework/install.

После завершения работы мастера установки можно перейти к настройке сервера.

Подготовить сертификаты сервера

OpenVPN предоставляет инструменты для подготовки сертификатов и других элементов в целях аутентификации и шифрования. Сертификаты требуются, в частности, для обеспечения безопасности канала связи между локальным сервером и облачным сервером. Инструменты управления сертификатами находятся в папке `%ProgramFiles%\OpenVPN\easy-rsa`.

На облачном компьютере откройте командную строку от имени администратора и введите следующие команды, чтобы настроить начальные значения для инструментов управления сертификатами:

```
cd "%ProgramFiles%\OpenVPN\easy-rsa"

init-config.bat
```

Этими командами в папке `easy-rsa` создается файл `vars.bat` с начальными значениями для построения сертификатов. Откройте файл `vars.bat` в Блокноте, чтобы просмотреть или изменить эти значения. В этом файле можно, например, задать значения полей сертификата, таких как `KEY_COUNTRY`, `KEY_PROVINCE`, `KEY_CITY` и т.д. Эти значения устанавливаются по умолчанию и могут быть изменены при построении сертификата.

Введите следующие команды для создания сертификата центра сертификации (CA):

```
vars.bat

clean-all.bat

build-ca.bat
```

При запросе ввода данных, можно принять значения по умолчанию или ввести другие значения для всех полей сертификата, кроме полей `Name` и `Common name`. В этих полях введите значение `ca`:

```
Common name: ca

Name: ca
```

Затем создайте сертификат и закрытый ключ для сервера OpenVPN. Для этого в командной строке введите следующую команду:

```
build-key-server.bat server
```

При запросе ввода данных, можно принять значения по умолчанию или ввести другие значения для всех полей сертификата, кроме полей `Name` и `Common name`. В этих полях введите значение `server`:

```
Common name: server

Name: server
```

Чтобы завершить настройку шифрования, подготовьте параметры Диффи-Хеллмана. Для этого в командной строке введите следующую команду:

```
build-dh.bat
```

В результате выполнения этих команд в папке `easy-rsa\keys` появятся следующие файлы: `ca.crt`, `server.crt`, `server.key`, `dh2048.pem`.

Настроить сервер OpenVPN

Сначала скопируйте подготовленные сертификаты (см. Подготовить сертификаты сервера) в папку конфигурации сервера OpenVPN. На облачном компьютере откройте командную строку от имени администратора и введите следующие команды:

```
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"
```

Затем выполните следующие команды, чтобы подготовить файл конфигурации сервера:

```
cd "%ProgramFiles%\OpenVPN\sample-config"
copy server.ovpn "%ProgramFiles%\OpenVPN\config"
```

Теперь нужно отредактировать файл конфигурации сервера, что проще всего сделать с помощью приложения Notepad++. Это приложение можно скачать и установить с сайта ninite.com/notepadplusplus. Установите Notepad++ и откройте файл конфигурации для редактирования:

```
cd "%ProgramFiles%\OpenVPN\config"
"%ProgramFiles%\Notepad++\notepad++.exe" server.ovpn
```

- или -

```
"%ProgramFiles(x86)%\Notepad++\notepad++.exe" server.ovpn
```

Отредактируйте файл конфигурации, устанавливая следующие значения параметров:

`local 0.0.0.0`

`port 80`

`proto tcp`

`;proto udp`
Поставьте точку с запятой в начале строки, чтобы отключить этот параметр.

`ifconfig-pool-persist ipp.txt`

`;tls-auth ta.key 0`
Поставьте точку с запятой в начале строки, чтобы отключить этот параметр.

`;explicit-exit-notify 1`
Поставьте точку с запятой в начале строки, чтобы отключить этот параметр.

Обратите внимание, что подсеть, из которой OpenVPN выбирает IP-адреса, задается параметром `server`:

```
server 10.8.0.0 255.255.255.0
```

При таком значении параметра серверу OpenVPN присваивается IP-адрес `10.8.0.1`, а остальные IP-адреса из этой подсети могут присваиваться клиентам OpenVPN.

Наконец, настройте сервер OpenVPN на автоматический запуск при запуске системы. Используйте консоль Службы (`services.msc`), чтобы установить для службы `OpenVPNService` тип запуска `Автоматически`. Затем запустите эту службу.

Настроить DeviceLock Enterprise Server

Настройте облачный сервер DeviceLock Enterprise Server следующим образом:

- Установите на сервере секретный ключ сертификата DeviceLock. Для этого используйте параметр **Сертификат DeviceLock** в узле Настройки сервера.
- Назначьте серверу фиксированный порт, например, порт `9133`. Для этого используйте параметр **TCP-порт** в узле Настройки сервера.

Настройка локальных серверов

На локальном компьютере необходимо установить и настроить клиент OpenVPN для подключения к серверу OpenVPN, работающему на облачном компьютере. При подключении сервер OpenVPN должен назначить клиенту определенный фиксированный IP-адрес. Кроме того, на локальном компьютере необходимо настроить сервер DeviceLock Enterprise Server для передачи журналов DeviceLock на облачный сервер.

В этом разделе рассматриваются следующие задачи по настройке локального сервера:

- Установить OpenVPN
- Подготовить клиентский сертификат и IP-адрес
- Настроить клиент OpenVPN
- Настроить DeviceLock Enterprise Server
- Тест: Подключить консоль к облачному серверу

Установить OpenVPN

Загрузите исполняемый файл установки OpenVPN для Windows с сайта openvpn.net/community-downloads (файл .exe). Запустите этот файл и следуйте инструкциям мастера установки:

- Установите все компоненты, за исключением **EasyRSA 2 Certificate Management Scripts**. На клиентских компьютерах этот компонент не используется.
- Примите папку установки по умолчанию, `%ProgramFiles%\OpenVPN`. В этой папке будет также храниться конфигурация клиента OpenVPN.
- При появлении запроса согласитесь установить программное обеспечение устройства TAP. Это виртуальное сетевое устройство обеспечивает соединение и обмен данными между клиентом и сервером OpenVPN.
- Для OpenVPN требуется Microsoft .NET Framework 4.0 или более поздней версии. По запросу мастера установите последнюю версию .NET Framework. Инструкции по установке см. в статье Microsoft по адресу docs.microsoft.com/dotnet/framework/install.

После завершения работы мастера установки можно перейти к настройке клиента.

Подготовить клиентский сертификат и IP-адрес

Для каждого клиента OpenVPN требуется сертификат с уникальным именем. Это может быть, например, имя локального компьютера.

Выполните следующие действия, чтобы создать сертификат для клиента OpenVPN:

1. На облачном компьютере, где установлен сервер OpenVPN, откройте командную строку от имени администратора.
2. В командной строке введите следующие команды:

   ```
   cd "%ProgramFiles%\OpenVPN\easy-rsa"
   vars.bat
   build-key.bat <имя компьютера>
   ```

   В последней команде `<имя компьютера>` обозначает имя локального компьютера, на котором будет работать клиент OpenVPN.

   При запросе ввода данных, можно принять значения по умолчанию или ввести другие значения для всех полей сертификата, кроме полей `Name` и `Common name`. В этих полях введите имя локального компьютера:

   ```
   Common name: <имя компьютера>
   Name: <имя компьютера>
   ```

После выполнения этих команд в папке `easy-rsa\keys` появятся файлы `<имя компьютера>.crt` и `<имя компьютера>.key`. Эти два файла вместе с файлом `ca.crt` необходимо скопировать в папку конфигурации клиента на локальном компьютере (`%ProgramFiles%\OpenVPN\config`).

Сервер OpenVPN должен назначать определенный фиксированный IP-адрес клиенту OpenVPN. Этот IP-адрес привязывается к имени клиентского сертификата, которое в нашем случае совпадает с именем локального компьютера.

Из-за известного ограничения драйвера TAP в случае маршрутизируемого IP-туннеля номер хоста в IP-адресе клиента должен быть таким, чтобы остаток от деления его на 4 равнялся 2. Например, если подсеть VPN, из которой OpenVPN выбирает адреса, имеет начальный IP-адрес `10.8.0.0` с маской сети `255.255.255.0` (задается директивой `server` в файле конфигурации сервера OpenVPN), то допустимый адрес клиента может быть `10.8.0.6`, `10.8.0.10`, `10.8.0.14`, `10.8.0.18` и так далее.

Выполните следующие действия, чтобы назначить фиксированный IP-адрес локальному компьютеру, на котором работает клиент OpenVPN:

1. На облачном компьютере, где установлен сервер OpenVPN, откройте командную строку от имени администратора.
2. В командной строке введите следующие команды:

   ```
   net stop OpenVPNService
   cd "%ProgramFiles%\OpenVPN\config"
   notepad ipp.txt
   ```

3. В файле `ipp.txt` добавьте строку, состоящую из имени клиентского сертификата, за которым следуют запятая и требуемый IP-адрес. Например:

   ```
   mycomp,10.8.0.6
   ```

Внимание:

- Для редактирования файла `ipp.txt` сервер OpenVPN должен быть остановлен. Это условие обеспечивается командой `net stop OpenVPNService`. После завершения редактирования запустите эту службу (например, введя `net start OpenVPNService` в командной строке).
- После запуска сервер OpenVPN обновляет файл `ipp.txt`, чтобы согласовать назначение IP-адреса клиента с требованиями драйвера TAP, вычитая 2 из фактического номера хоста. Например, для клиента с IP-адресом `10.8.0.6` в файле `ipp.txt` будет указан IP-адрес `10.8.0.4`.

Настроить клиент OpenVPN

При подготовке клиентского сертификата (см. Подготовить клиентский сертификат и IP-адрес) в папке `easy-rsa\keys` были созданы файлы `<имя компьютера>.crt` и `<имя компьютера>.key`. Скопируйте эти два файла вместе с файлом `ca.crt` в папку `%ProgramFiles%\OpenVPN\config` конфигурации клиента на локальном компьютере.

Затем на локальном компьютере откройте командную строку от имени администратора и введите следующие команды для подготовки файла конфигурации клиента:

```
cd "%ProgramFiles%\OpenVPN\sample-config"

copy client.ovpn "%ProgramFiles%\OpenVPN\config"
```

Теперь нужно отредактировать файл конфигурации клиента, что проще всего сделать с помощью приложения Notepad++. Это приложение можно скачать и установить с сайта ninite.com/notepadplusplus. Установите Notepad++ и откройте файл конфигурации для редактирования:

```
cd "%ProgramFiles%\OpenVPN\config"

"%ProgramFiles%\Notepad++\notepad++.exe" server.ovpn
```

- или -

```
"%ProgramFiles(x86)%\Notepad++\notepad++.exe" server.ovpn
```

Отредактируйте файл конфигурации, устанавливая следующие значения параметров:

`proto tcp`

`;proto udp`
Поставьте точку с запятой в начале строки, чтобы отключить этот параметр.

`remote <публичный IP-адрес облачного компьютера> 80`
Пример: `remote 212.46.5.117 80`

`cert <имя компьютера>.crt`

`key <имя компьютера>.key`

`;tls-auth ta.key 1`
Поставьте точку с запятой в начале строки, чтобы отключить этот параметр.

Наконец, настройте клиент OpenVPN на автоматический запуск при запуске системы. Используйте консоль Службы (`services.msc`), чтобы установить для службы `OpenVPNService` тип запуска `Автоматически`. Затем запустите эту службу.

Настроить DeviceLock Enterprise Server

Настройте локальный сервер DeviceLock Enterprise Server следующим образом:

- Назначьте серверу фиксированный порт, например, порт `9133`. Для этого используйте параметр **TCP-порт** в узле Настройки сервера.
- Направьте трафик консолидации с локального сервера DeviceLock Enterprise Server на сервер OpenVPN облачного компьютера и настройте аутентификацию по сертификату:
  1. Дважды щелкните параметр **Консолидация журналов** узле Настройки сервера.
  2. В поле **Сервер консолидации** появившегося диалогового окна введите IP-адрес сервера OpenVPN.

     Это адрес сервера из подсети OpenVPN, определенной параметром `server` в файле конфигурации сервера. Так, если для этого параметра установлено значение `10.8.0.0 255.255.255.0`, IP-адрес сервера OpenVPN будет `10.8.0.1`.
  3. Нажмите кнопку рядом с полем **Сервер консолидации** и в открывшемся диалоговом окне предоставьте открытый ключ сертификата DeviceLock. Это должен быть сертификат, секретный ключ которого установлен на облачном сервере.
- Настройте отправку на облачный сервер клиентского IP-адреса и номера порта:
  1. В редакторе реестра Windows (regedit) откройте следующий раздел реестра: `HKLM\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer`
  2. В этом разделе реестра создайте параметр со следующими настройками:
     - Имя: `SlaveRemoteAddress`
     - Тип: `REG_SZ`
     - Значение: IP-адрес локального клиента OpenVPN (например, `10.8.0.6`), за которым следует двоеточие и номер порта, назначенного серверу DeviceLock Enterprise Server на данном локальном компьютере. Пример: `10.8.0.6:9133`

     Локальный сервер отправит это значение на облачный сервер при отправке запроса на консолидацию. Таким образом, облачному серверу станет известен IP-адрес и порт для связи с данным локальным сервером.

Тест: Подключить консоль к облачному серверу

После настройки OpenVPN можно проверить его, подключив локальную консоль к облачному серверу. Запустите консоль DeviceLock Management Console на локальном компьютере и подключитесь к серверу DeviceLock Enterprise Server, работающему в облаке:

1. Запустите консоль DeviceLock Management Console на локальном компьютере.
2. В дереве консоли щелкните правой кнопкой мыши узел **DeviceLock Enterprise Server** и выберите команду **Подключиться**.
3. В появившемся диалоговом окне нажмите кнопку **Другим компьютером**.
4. В поле рядом с кнопкой **Другим компьютером** введите IP-адрес сервера OpenVPN на облачном компьютере, а затем заключенный в скобки номер порта, назначенного серверу DeviceLock Enterprise Server. Пример: `10.8.0.1[9133]`
5. Нажмите **OK** и подождите, пока консоль установит подключение.
6. Если консоль запросит имя пользователя и пароль, введите имя и пароль учетной записи пользователя с достаточными правами для доступа к серверу DeviceLock Enterprise Server на облачном компьютере.

При таком VPN-подключении консоль обменивается данными с облачным сервером, отправляя RPC-запросы локальному клиенту OpenVPN. Клиент отсылает запросы облачному серверу OpenVPN, который, в свою очередь, передает их на сервер DeviceLock Enterprise Server.

17

Приложение: Примеры

В этой главе:

Примеры разрешений и правил аудита для устройств

Примеры разрешений для протоколов

Примеры контентно-зависимых правил

Примеры правил IP-файрвола

Примеры разрешений и правил аудита для устройств

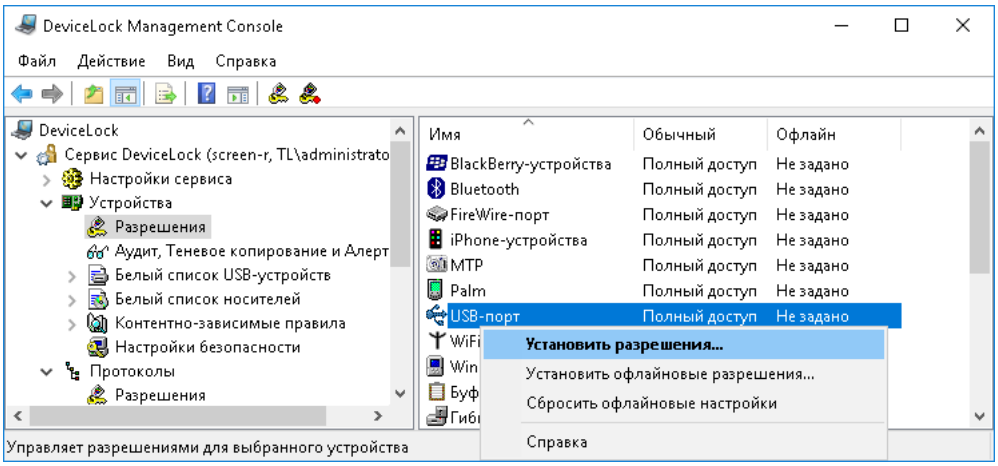
Следующие примеры показывают, как правильно устанавливать разрешения, правила аудита и теневого копирования в DeviceLock.

Во всех примерах используется консоль DeviceLock Management Console, подключенная к компьютеру, на котором работает сервис DeviceLock. Подробнее о консоли DeviceLock Management Console см. в разделе Консоли и инструменты DeviceLock данного руководства.

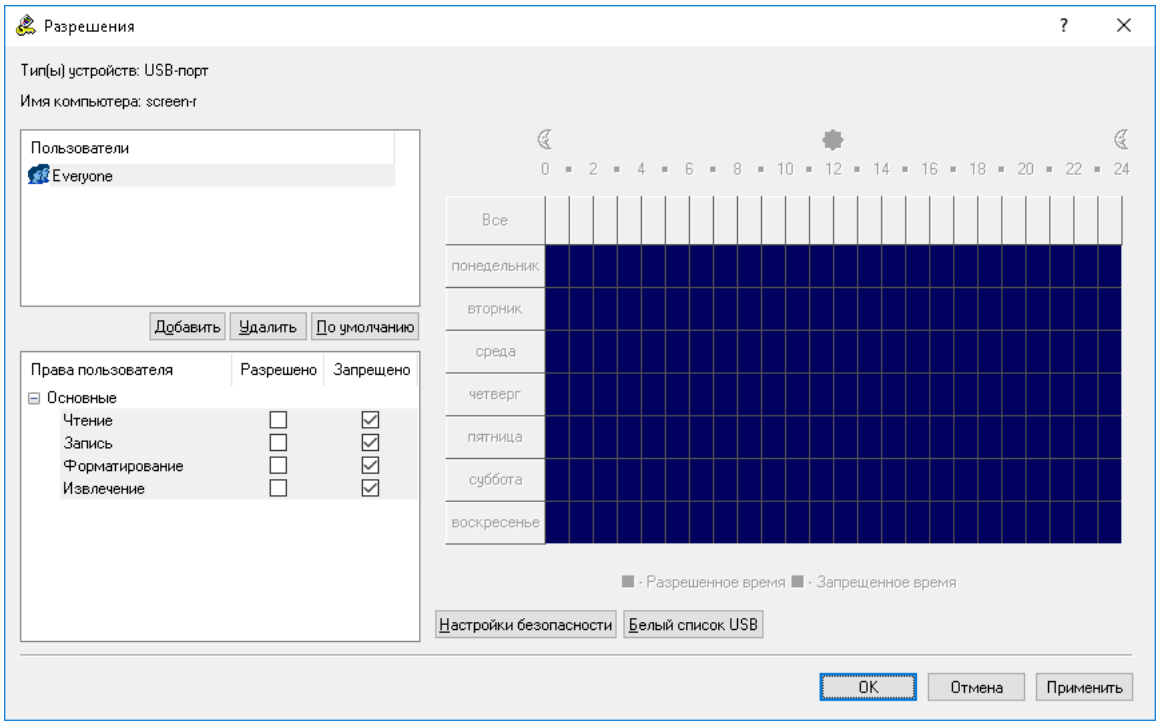
Примеры разрешений

Для всех пользователей запрещены все USB-устройства, кроме клавиатуры и мыши:

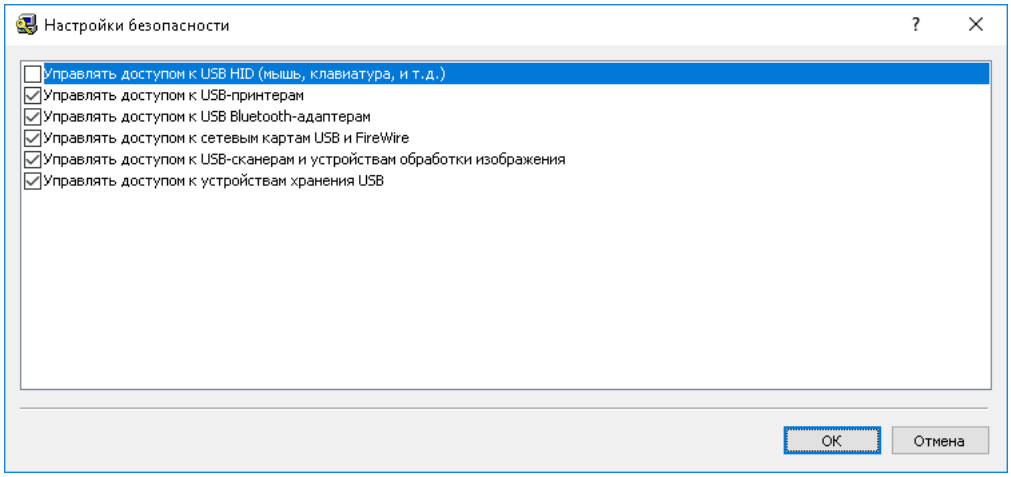
1. Выберите запись **USB-порт** из списка типов устройств в разделе **Разрешения**, затем выберите **Установить разрешения** из контекстного меню, доступного по нажатию правой кнопки мыши.



2. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения**, добавьте учетную запись **Все** (Everyone), нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя, выделите запись **Все** и отключите для нее все права в списке **Права пользователя**.



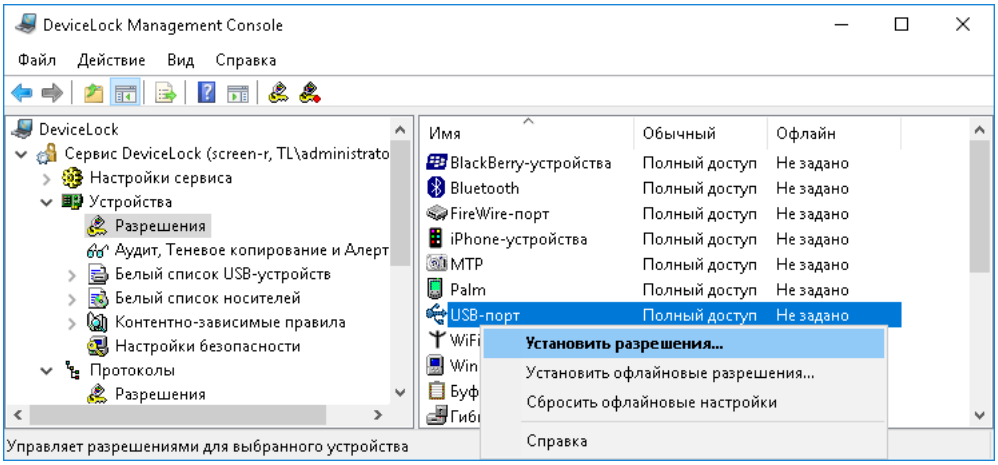
3. Нажмите кнопку **Настройки безопасности** в диалоговом окне **Разрешения**, затем снимите флажок **Управлять доступом к USB HID (мышь, клавиатура, и т.д.)** в появившемся диалоговом окне **Настройки безопасности**.



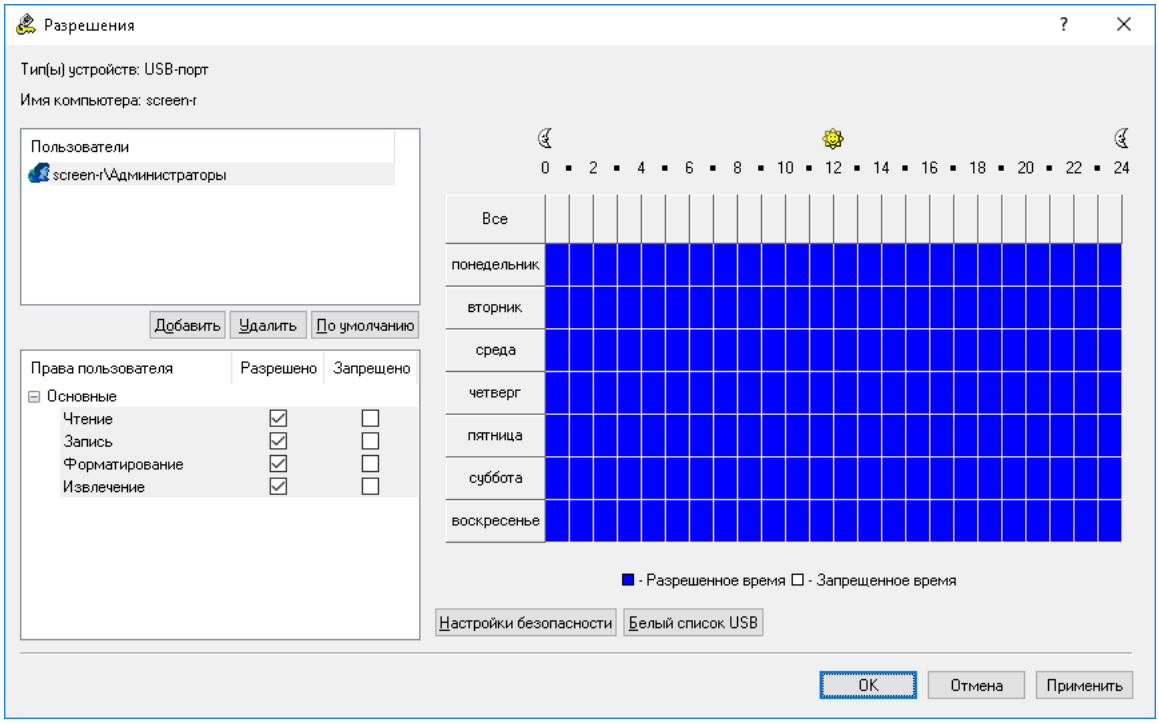
4. Нажмите **OK**, чтобы закрыть диалоговое окно **Настройки безопасности**, нажмите **OK**, чтобы применить настройки и закрыть диалоговое окно **Разрешения**, затем нажмите **Да**, чтобы подтвердить, что вы действительно хотите запретить доступ к USB-порту для всех.

Для всех пользователей запрещены все USB-устройства, кроме клавиатуры и мыши, но Администраторы могут использовать любые USB-устройства:

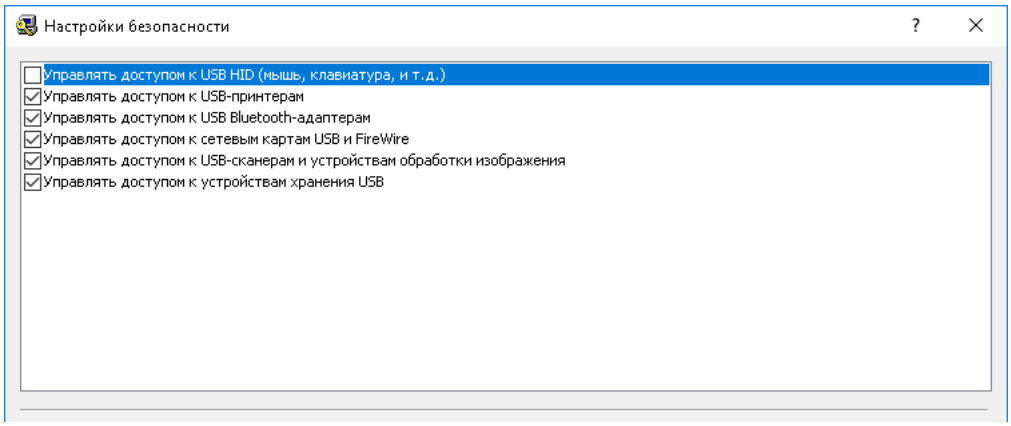
1. Выберите запись **USB-порт** из списка типов устройств в разделе **Разрешения**, затем выберите **Установить разрешения** из контекстного меню, доступного по нажатию правой кнопки мыши.



2. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения**, добавьте группу **Администраторы**, нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, выделите запись **Администраторы** и включите для нее все права в списке **Права пользователя**.



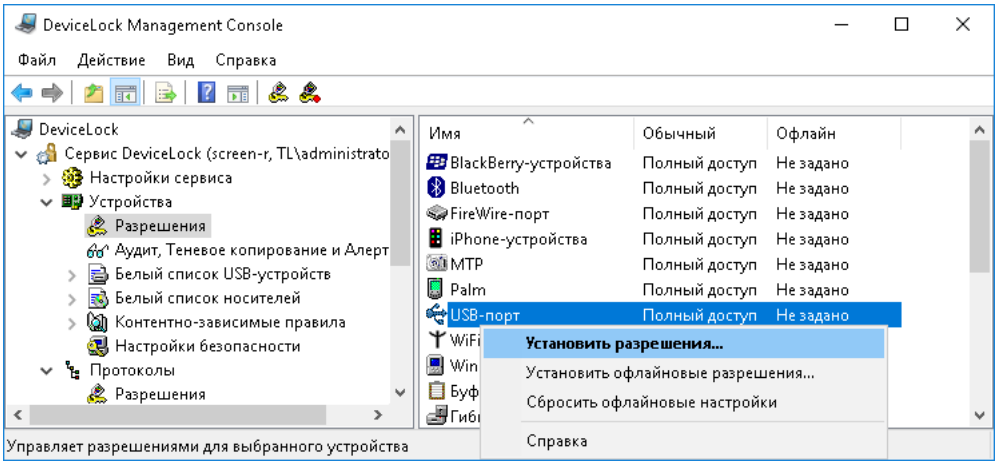
3. Нажмите кнопку **Настройки безопасности** в диалоговом окне **Разрешения**, затем снимите флажок **Управлять доступом к USB HID (мышь, клавиатура, и т.д.)** в появившемся диалоговом окне **Настройки безопасности**.



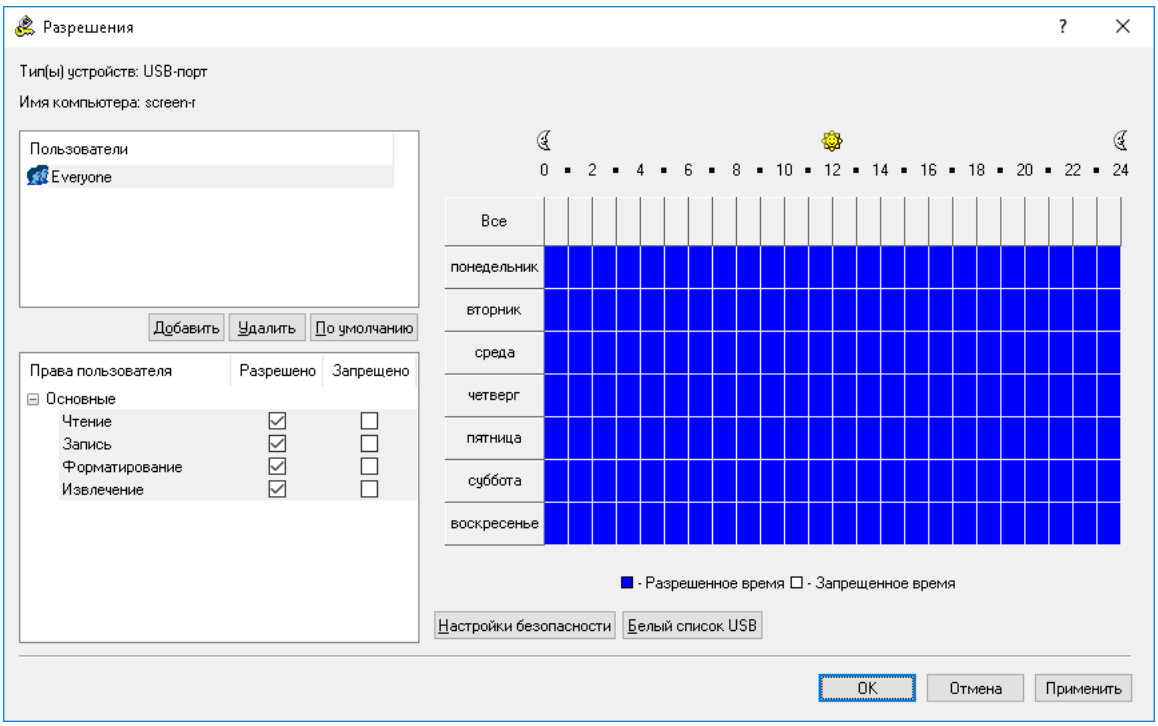
4. Нажмите **OK**, чтобы закрыть диалоговое окно **Настройки безопасности**, затем нажмите **OK**, чтобы применить настройки и закрыть диалоговое окно **Разрешения**,

Для всех пользователей запрещены все устройства хранения данных за исключением внутренних жестких дисков, но все USB-устройства, не предназначенные для хранения данных - разрешены:

1. Выберите запись **USB-порт** из списка типов устройств в разделе **Разрешения**, затем выберите **Установить разрешения** из контекстного меню, доступного по нажатию правой кнопки мыши.

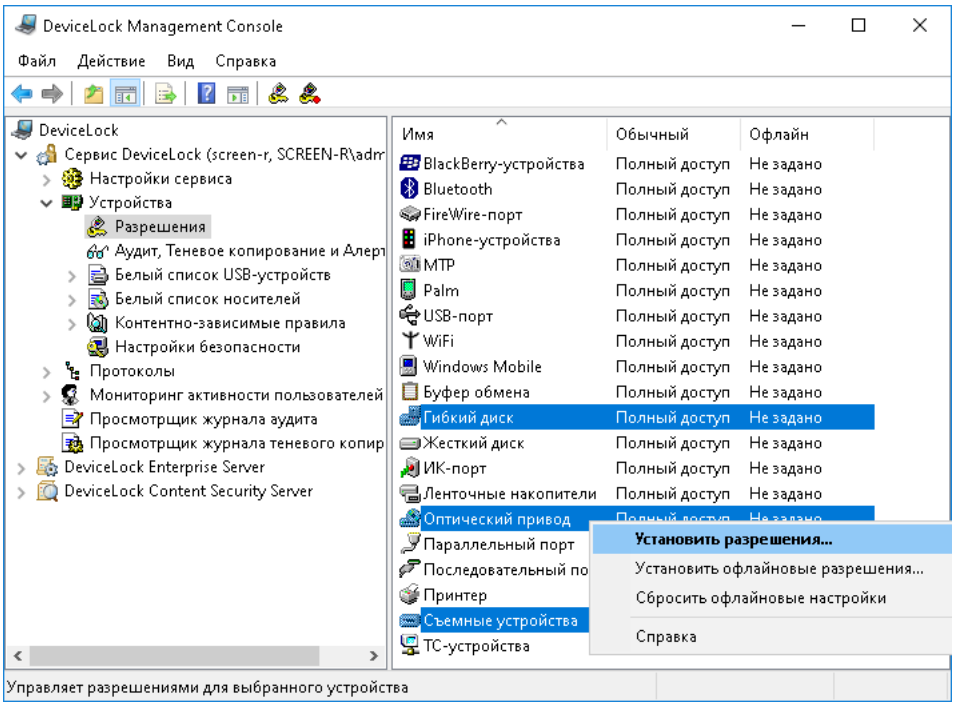


2. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения**, добавьте учетную запись **Все** (Everyone), нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя, выделите запись **Все** и включите для нее все права в списке **Права пользователя**.

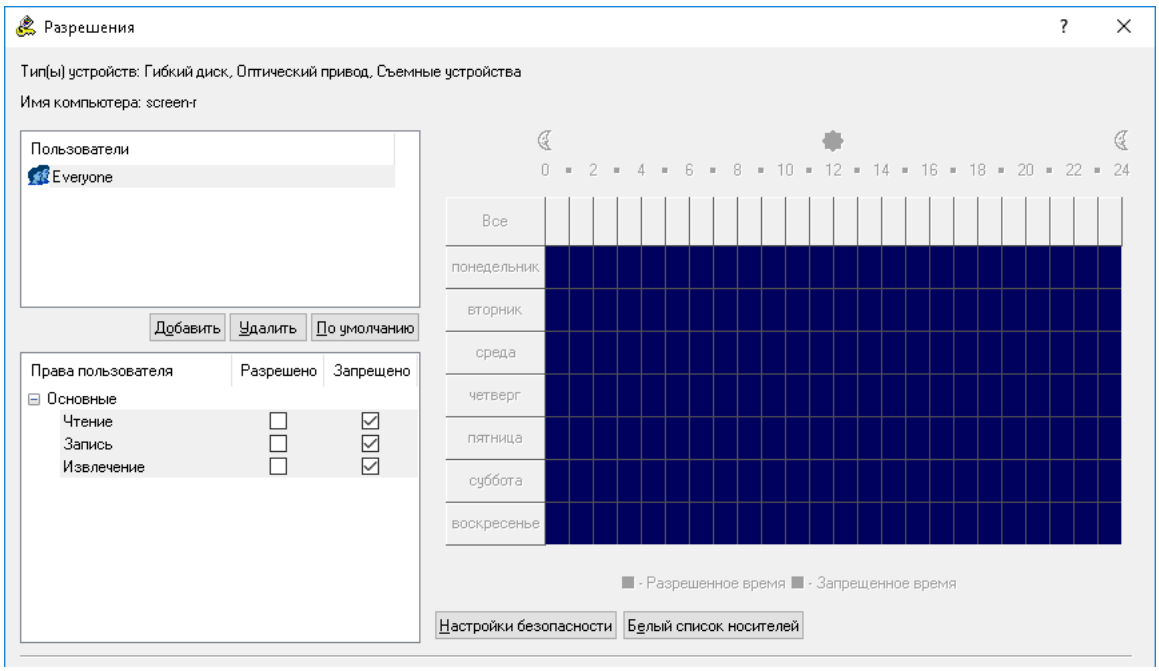


3. Нажмите **OK**, чтобы применить настройки и закрыть диалоговое окно **Разрешения**.

4. Выберите записи **Гибкий диск**, **Оптический привод** и **Съемные устройства** из списка типов устройств в разделе **Разрешения**, затем выберите **Установить разрешения** из контекстного меню, доступного по нажатию правой кнопки мыши.



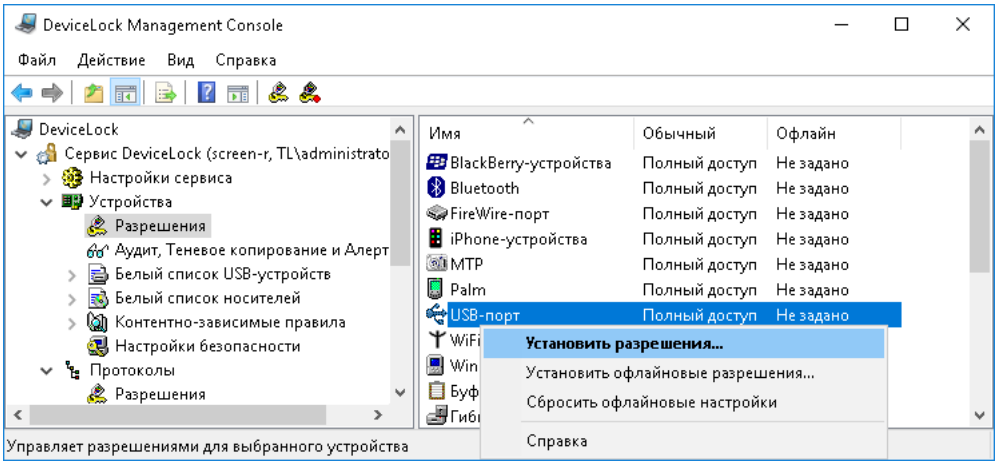
5. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения**, добавьте учетную запись **Все** (Everyone), нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя, выделите запись **Все** и отключите для нее все права в списке **Права пользователя**.



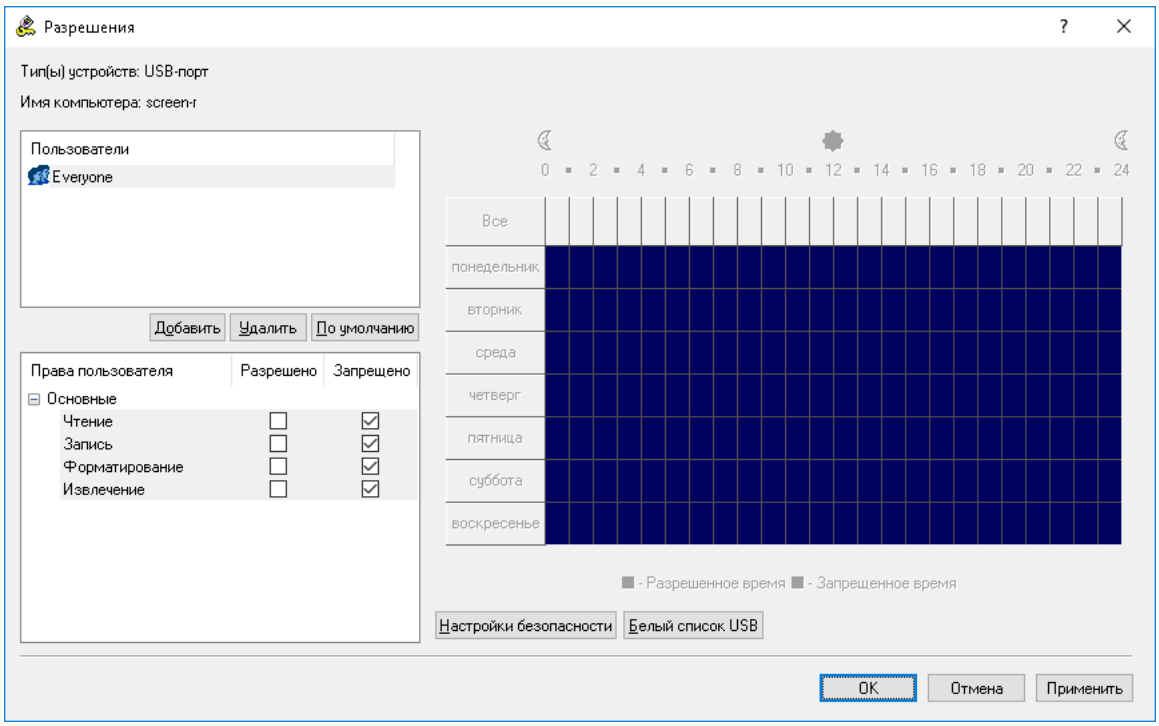
6. Нажмите **OK**, чтобы применить настройки и закрыть диалоговое окно **Разрешения**, затем нажмите **Да**, чтобы подтвердить, что вы действительно хотите запретить доступ к этим устройствам для всех.

Для всех пользователей запрещены все USB-устройства, кроме клавиатуры и мыши, но Администраторы могут использовать определенную модель USB-флешки:

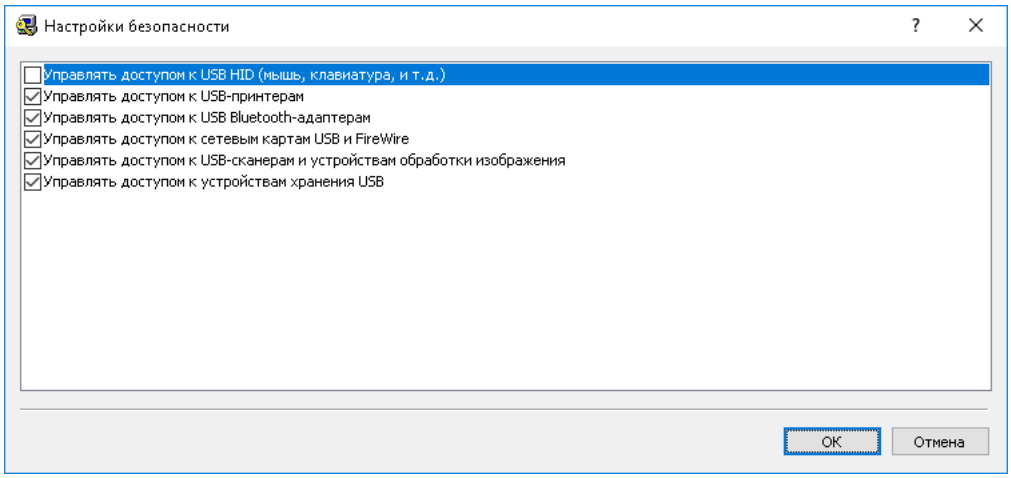
1. Выберите запись **USB-порт** из списка типов устройств в разделе **Разрешения**, затем выберите **Установить разрешения** из контекстного меню, доступного по нажатию правой кнопки мыши.



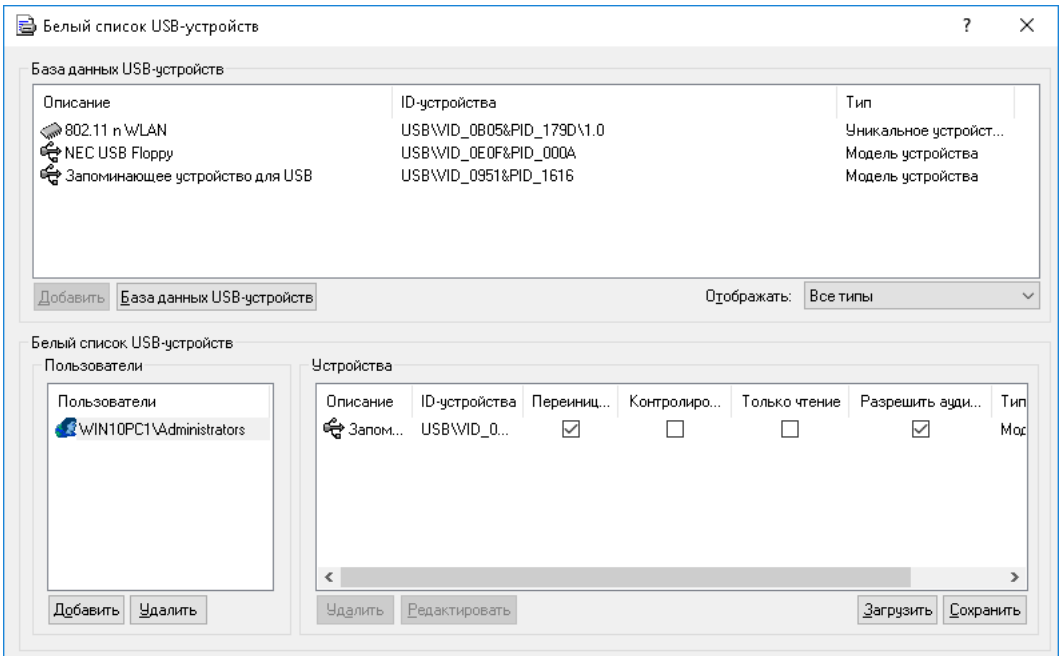
2. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения**, добавьте учетную запись **Все** (Everyone), нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя, выделите запись **Все** и отключите для нее все права в списке **Права пользователя**.



3. Нажмите кнопку **Настройки безопасности** в диалоговом окне **Разрешения**, затем снимите флажок **Управлять доступом к USB HID (мышь, клавиатура, и т.д.)** в появившемся диалоговом окне **Настройки безопасности**.



4. Нажмите **OK**, чтобы закрыть диалоговое окно **Настройки безопасности**.
5. Нажмите кнопку **Белый список USB** в диалоговом окне **Разрешения**.
6. В появившемся диалоговом окне **Белый список USB-устройств** нажмите кнопку **Добавить** под списком **Пользователи**, добавьте группу **Администраторы**, нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, и выделите запись **Администраторы**.



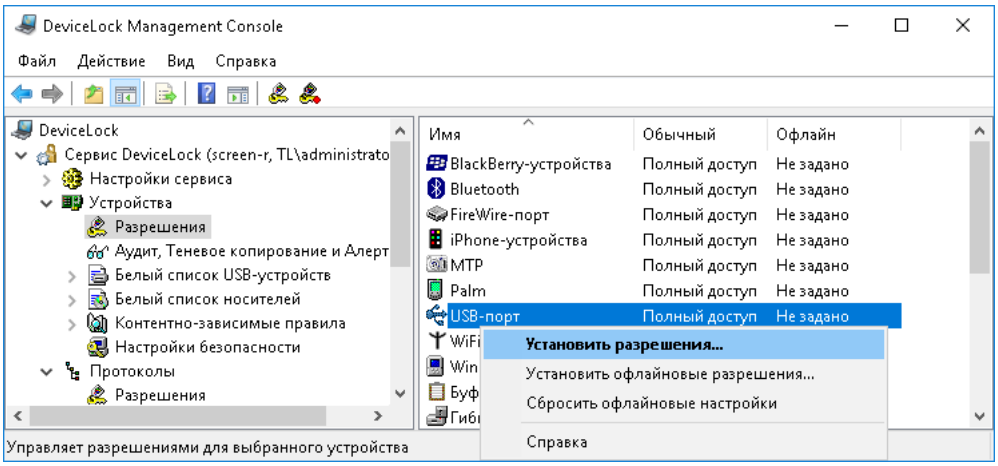
7. Выделите нужную модель устройства в списке **База данных USB-устройств**, затем нажмите кнопку **Добавить** под этим списком.

   Если в списке **База данных USB-устройств** нет записей, то нажмите кнопку **База данных USB-устройств** под этим списком и затем добавьте устройства, как описано в разделе База данных USB-устройств данного руководства. Когда закончите добавлять устройства в базу данных, нажмите **OK**, чтобы сохранить базу данных и закрыть диалоговое окно **База данных USB-устройств**.

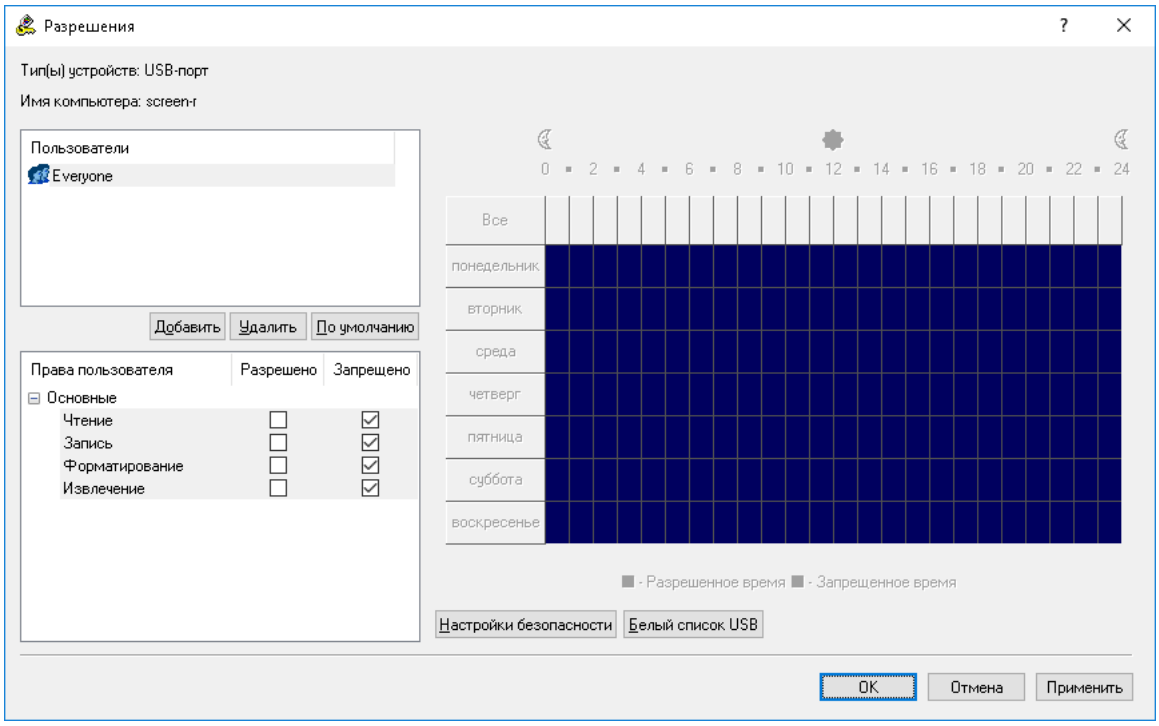
8. Нажмите **OK**, чтобы сохранить изменения в белом списке и закрыть диалоговое окно **Белый список USB-устройств**, нажмите **OK**, чтобы применить настройки и закрыть диалоговое окно **Разрешения**, затем нажмите **Да**, чтобы подтвердить, что вы действительно хотите запретить доступ к USB для всех.

Для всех пользователей запрещены все USB-устройства, кроме клавиатуры и мыши, но Администраторы могут использовать определенный экземпляр USB-флешки:

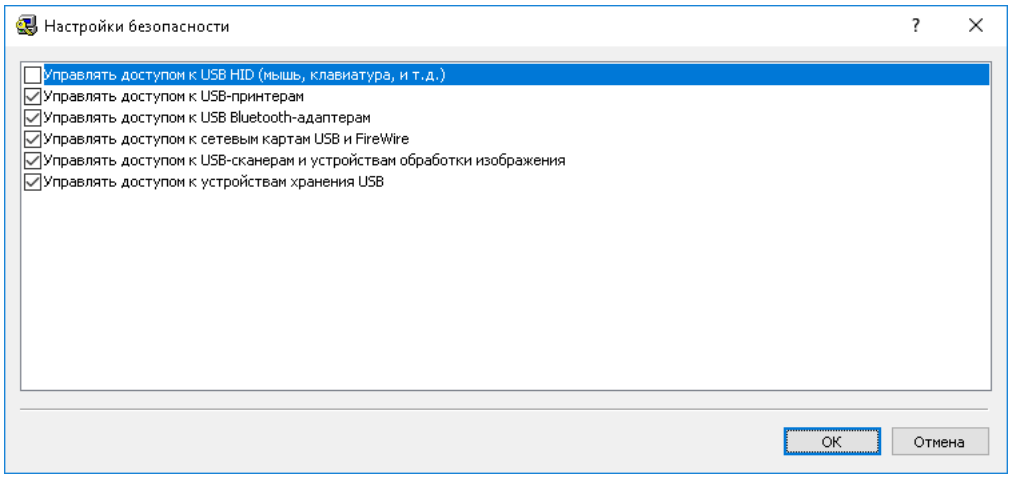
1. Выберите запись **USB-порт** из списка типов устройств в разделе **Разрешения**, затем выберите **Установить разрешения** из контекстного меню, доступного по нажатию правой кнопки мыши.



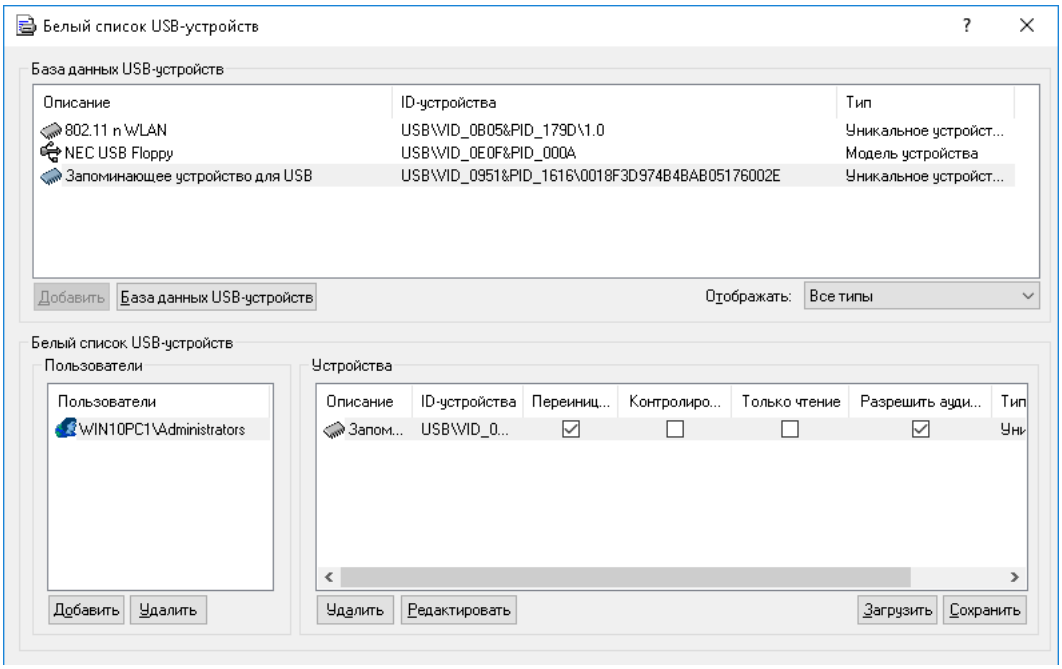
2. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения**, добавьте учетную запись **Все** (Everyone), нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя, выделите запись **Все** и отключите для нее все права в списке **Права пользователя**.



3. Нажмите кнопку **Настройки безопасности** в диалоговом окне **Разрешения**, затем снимите флажок **Управлять доступом к USB HID (мышь, клавиатура, и т.д.)** в появившемся диалоговом окне **Настройки безопасности**.



4. Нажмите **OK**, чтобы закрыть диалоговое окно **Настройки безопасности**.
5. Нажмите кнопку **Белый список USB** в диалоговом окне **Разрешения**.
6. В появившемся диалоговом окне **Белый список USB-устройств** нажмите кнопку **Добавить** под списком **Пользователи**, добавьте группу **Администраторы**, нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, и выделите запись **Администраторы**.



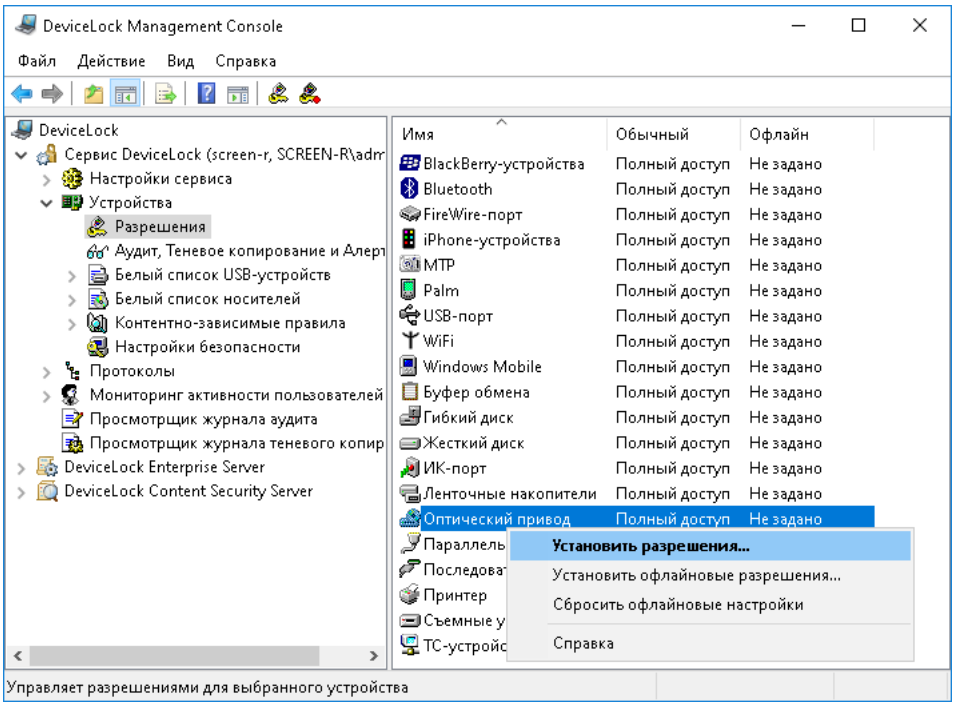
7. Выберите нужное уникальное устройство в списке **База данных USB-устройств**, затем нажмите кнопку **Добавить** под этим списком.

   Если в списке **База данных USB-устройств** нет записей, то нажмите кнопку **База данных USB-устройств** под этим списком и затем добавьте устройства, как описано в разделе База данных USB-устройств данного руководства. Когда закончите добавлять устройства в базу данных, нажмите **OK**, чтобы сохранить базу данных и закрыть диалоговое окно **База данных USB-устройств**.

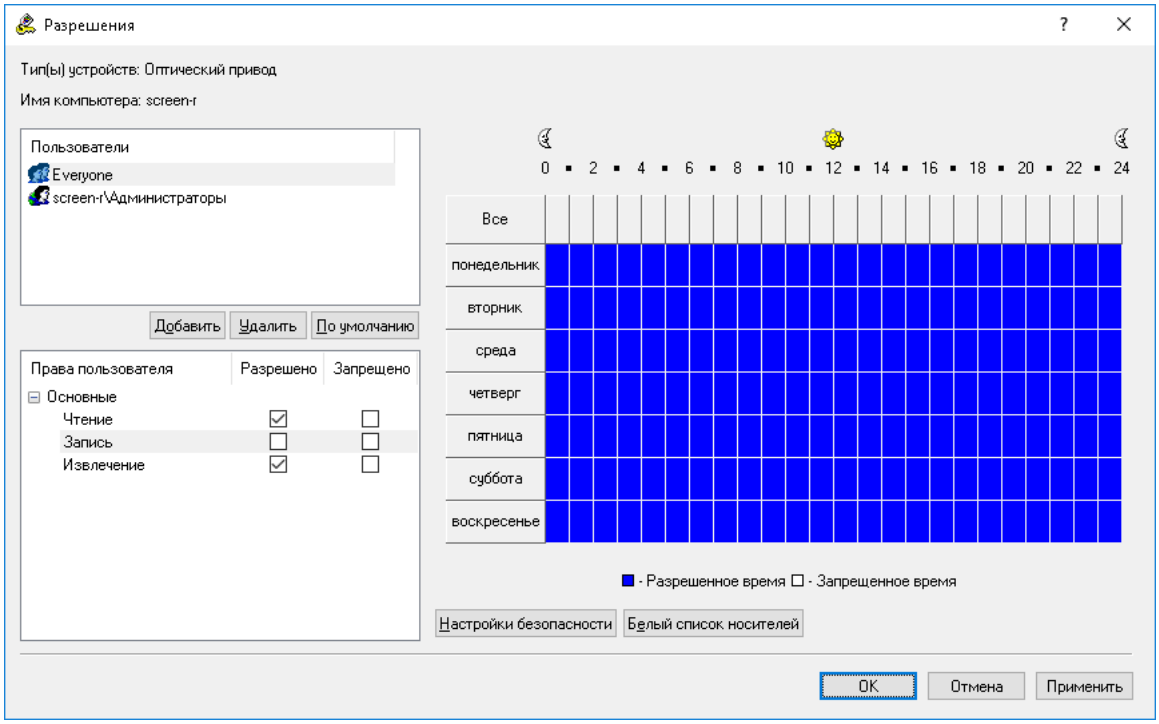
8. Нажмите **OK**, чтобы сохранить изменения в белом списке и закрыть диалоговое окно **Белый список USB-устройств**, нажмите **OK**, чтобы применить настройки и закрыть диалоговое окно **Разрешения**, затем нажмите **Да**, чтобы подтвердить, что вы действительно хотите запретить доступ к USB для всех.

Для всех пользователей все приводы CD / DVD / BD доступны только для чтения, но Администраторы могут записывать CD, DVD и BD-диски:

1. Выберите запись **Оптический привод** из списка типов устройств в разделе **Разрешения**, затем выберите **Установить разрешения** из контекстного меню, доступного по нажатию правой кнопки мыши.



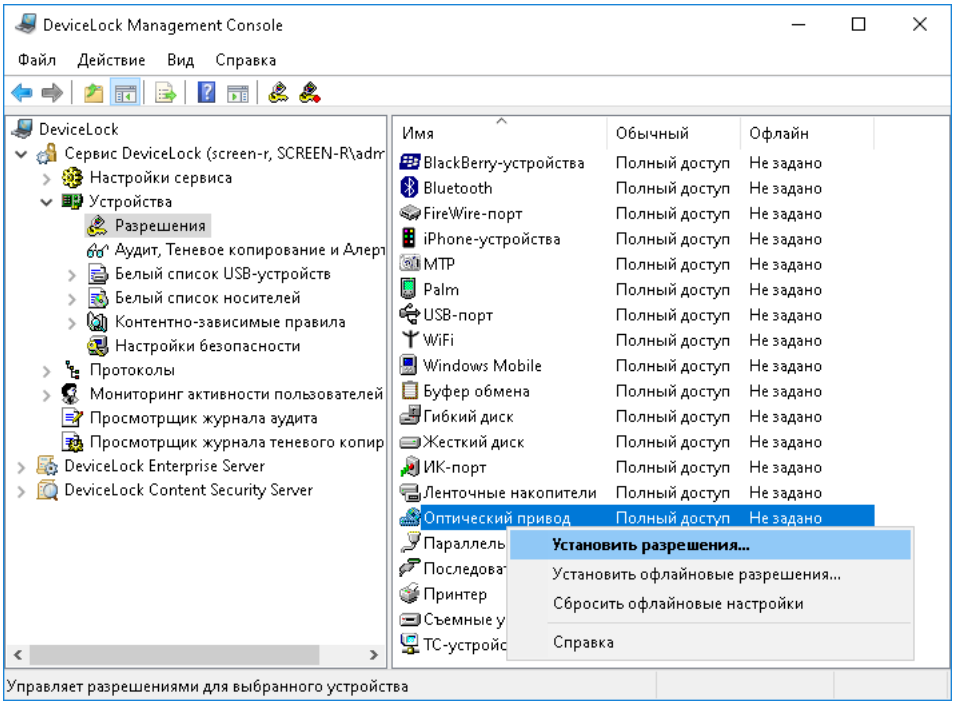
2. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения** и добавьте группу **Администраторы** (введите имя вручную или выберите его из полного списка имен). Нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, выберите запись **Администраторы** и включите все права в списке **Права пользователя**.
3. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения**, добавьте учетную запись **Все** (Everyone), нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, выделите запись **Все** и отключите для нее право **Запись** в списке **Права пользователя**.



4. Нажмите **OK**, чтобы применить изменения и закрыть диалоговое окно **Разрешения**.

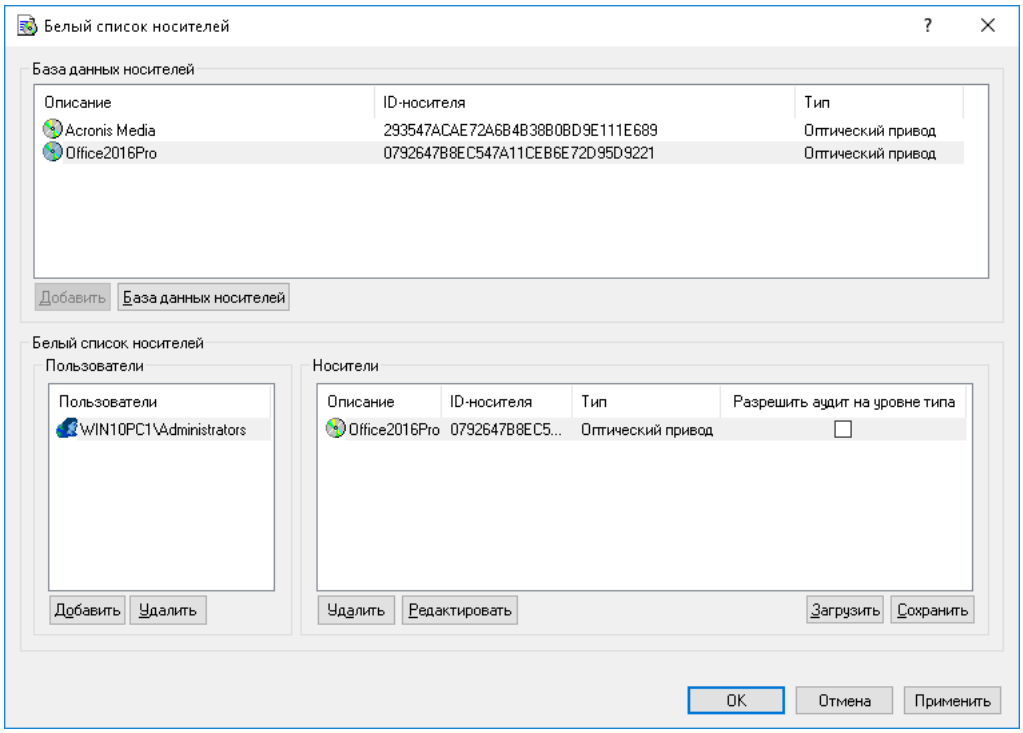
Для всех пользователей запрещены все приводы CD / DVD / BD, но Администраторы могут читать определенный оптический диск:

1. Выберите **Оптический привод** из списка типов устройств в разделе **Разрешения**, затем выберите **Установить разрешения** из контекстного меню, доступного по нажатию правой кнопки мыши.



2. Нажмите кнопку **Добавить** в диалоговом окне **Разрешения** и добавьте учетную запись **Все** (Everyone). Нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, выберите запись **Все** и отключите все права в списке **Права пользователя**.
3. Нажмите кнопку **Белый список носителей** в диалоговом окне **Разрешения**.

4. В появившемся диалоговом окне **Белый список носителей** нажмите кнопку **Добавить** под списком **Пользователи**, добавьте группу **Администраторы**, нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, и выделите запись **Администраторы**.



5. Выберите нужный носитель в списке **База данных носителей**, затем нажмите кнопку **Добавить** под этим списком

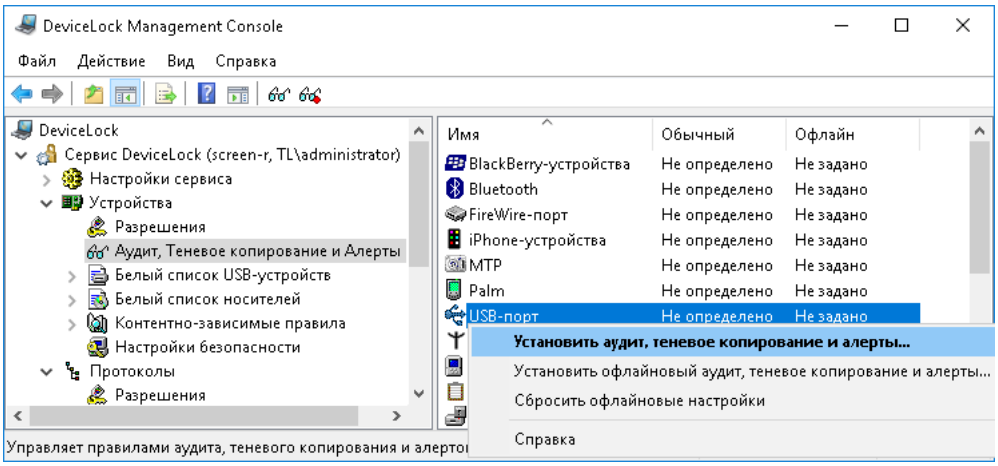
   Если в списке **База данных носителей** нет записей, то нажмите кнопку **База данных носителей** под этим списком и затем добавьте носители, как описано в разделе База данных носителей данного руководства. Когда вы закончите добавлять носители в базу данных, нажмите **OK**, чтобы сохранить базу данных и закрыть диалоговое окно **База данных носителей**.

6. Нажмите **OK**, чтобы сохранить изменения в белом списке и закрыть диалоговое окно **Белый список носителей**. Нажмите **OK**, чтобы применить настройки и закрыть диалоговое окно **Разрешения**, затем нажмите **Да**, чтобы подтвердить, что вы действительно хотите запретить доступ к CD/DVD/BD-приводам для всех.

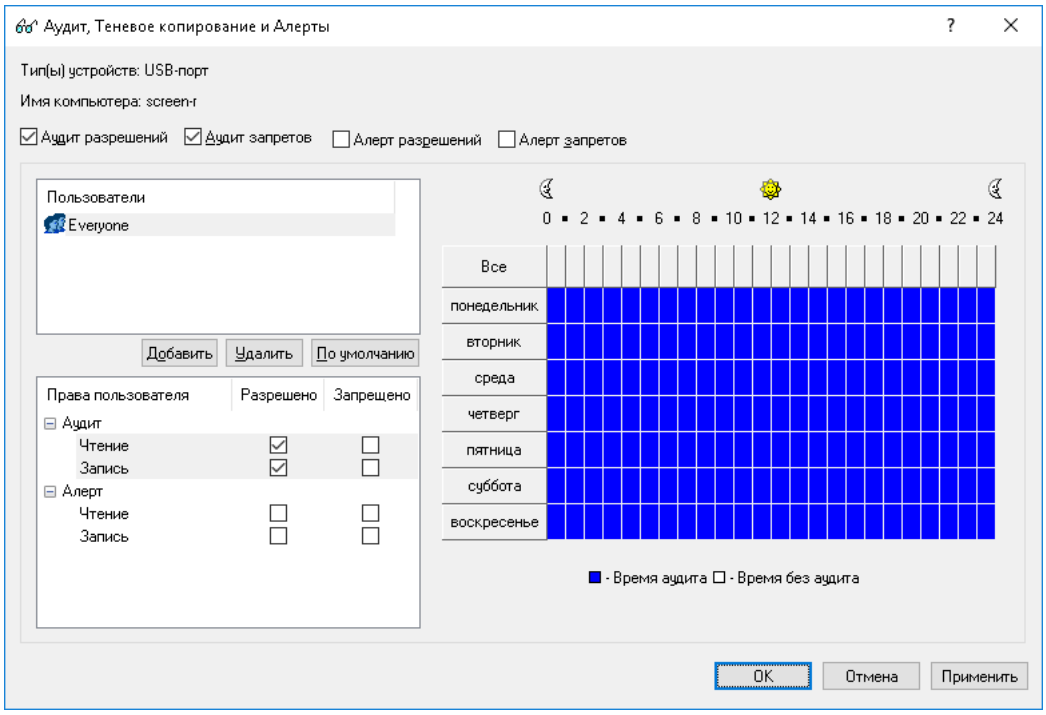
Примеры правил аудита и теневого копирования

Протоколируются события подключения, отключения и попытки доступа для всех USB-устройств для всех пользователей:

1. Выберите запись **USB-порт** из списка типов устройств в разделе **Аудит, Теневое копирование и Алерты**, затем выберите команду **Установить аудит, теневое копирование и алерты** из контекстного меню, доступного по нажатию правой кнопки мыши.



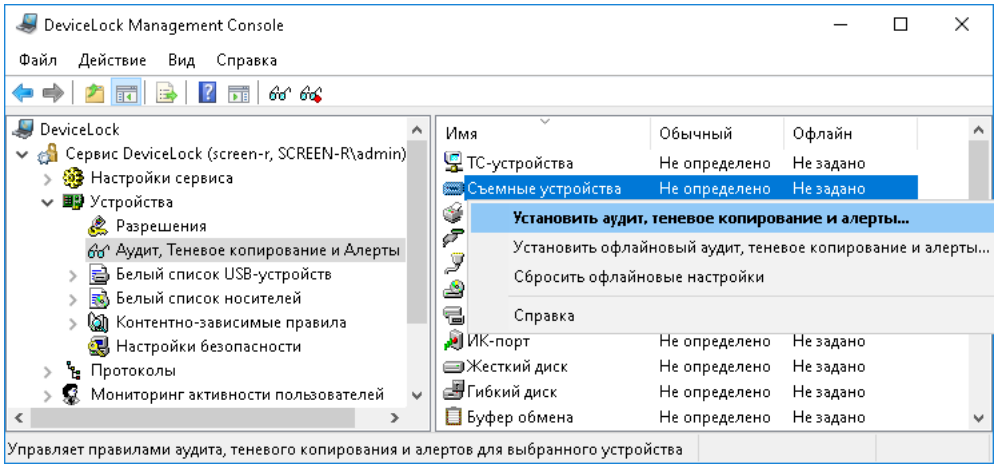
2. Нажмите кнопку **Добавить** в диалоговом окне **Аудит, Теневое копирование и Алерты**, добавьте учетную запись **Все** (Everyone), нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, выделите запись **Все** и включите для нее права аудита **Чтение** и **Запись** в списке **Права пользователя**.



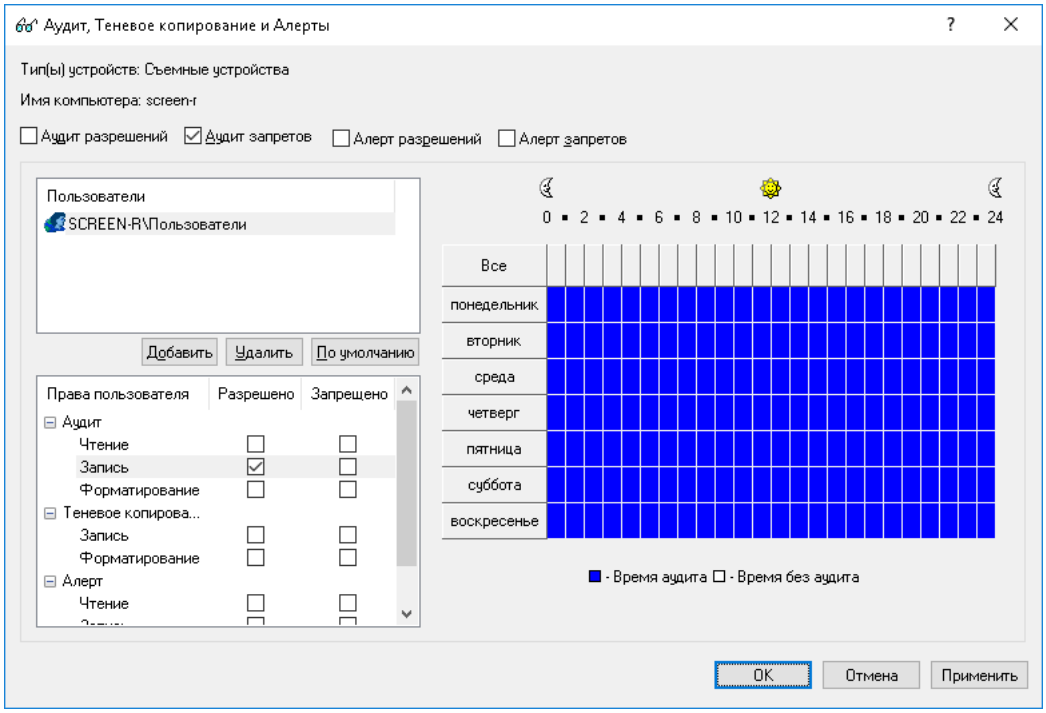
3. Установите флажки **Аудит разрешений** и **Аудит запретов**, находящиеся в верхней части диалогового окна **Аудит, Теневое копирование и Алерты**, затем нажмите **OK**, чтобы применить настройки и закрыть это диалоговое окно.

Протоколируются имена файлов и директорий только при запрещенных попытках записи на сменные накопители для группы Пользователи:

1. Выберите запись **Съемные устройства** из списка типов устройств в разделе **Аудит, Теневое копирование и Алерты**, затем выберите команду **Установить аудит, теневое копирование и алерты** из контекстного меню, доступного по нажатию правой кнопки мыши.



2. Нажмите кнопку **Добавить** в диалоговом окне **Аудит, Теневое копирование и Алерты**, добавьте группу **Пользователи**, нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, выделите запись **Пользователи** и включите для нее только право аудита **Запись** в списке **Права пользователя**.

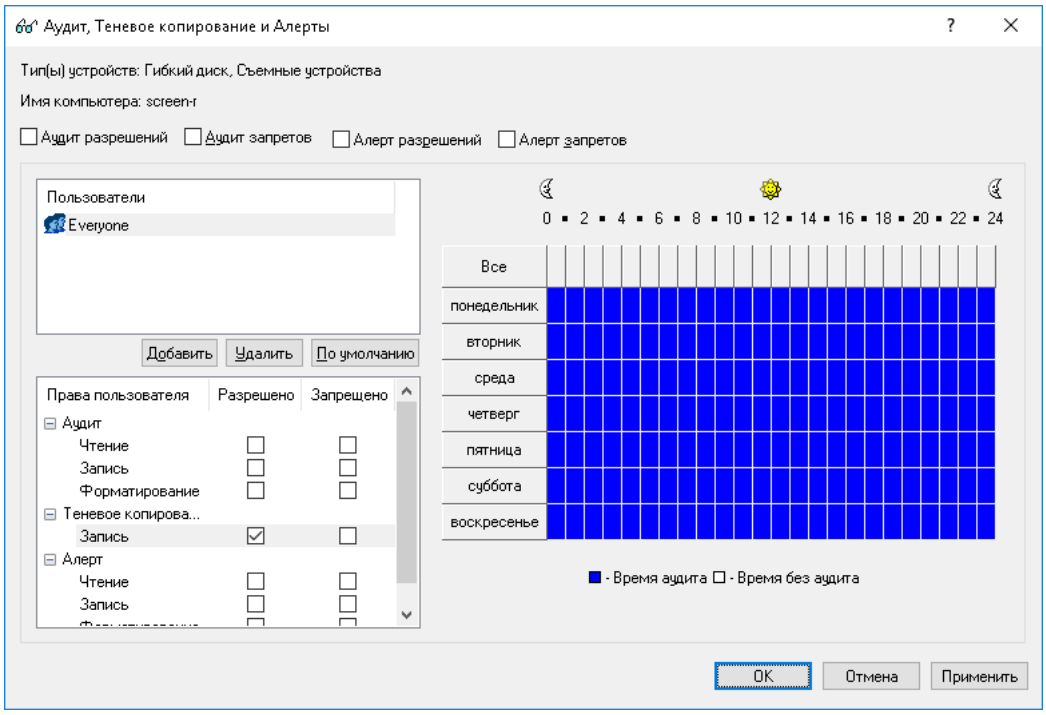


3. Установите только флажок **Аудит запретов** находящийся в верхней части диалогового окна **Аудит, Теневое копирование и Алерты**, затем нажмите **OK**, чтобы применить настройки и закрыть это диалоговое окно.

4. Включите параметр **Аудит операций с папками** в области **Аудит и теневое копирование** раздела **Настройки сервиса**.

Включено теневое копирование для всех данных, записываемых на сменные носители и дискеты любым пользователем:

1. Выберите записи **Гибкий диск** и **Съемные устройства** из списка типов устройств в разделе **Аудит, Теневое копирование и Алерты**, затем выберите команду **Установить аудит, теневое копирование и алерты** из контекстного меню, доступного по нажатию правой кнопки мыши.
2. Нажмите кнопку **Добавить** в диалоговом окне **Аудит, Теневое копирование и Алерты**, добавьте учетную запись **Все** (Everyone), нажмите **OK**, чтобы закрыть диалоговое окно выбора пользователя или группы, выделите запись **Все**, отключите для нее все права аудита и включите только право теневого копирования **Запись** в списке **Права пользователя**.

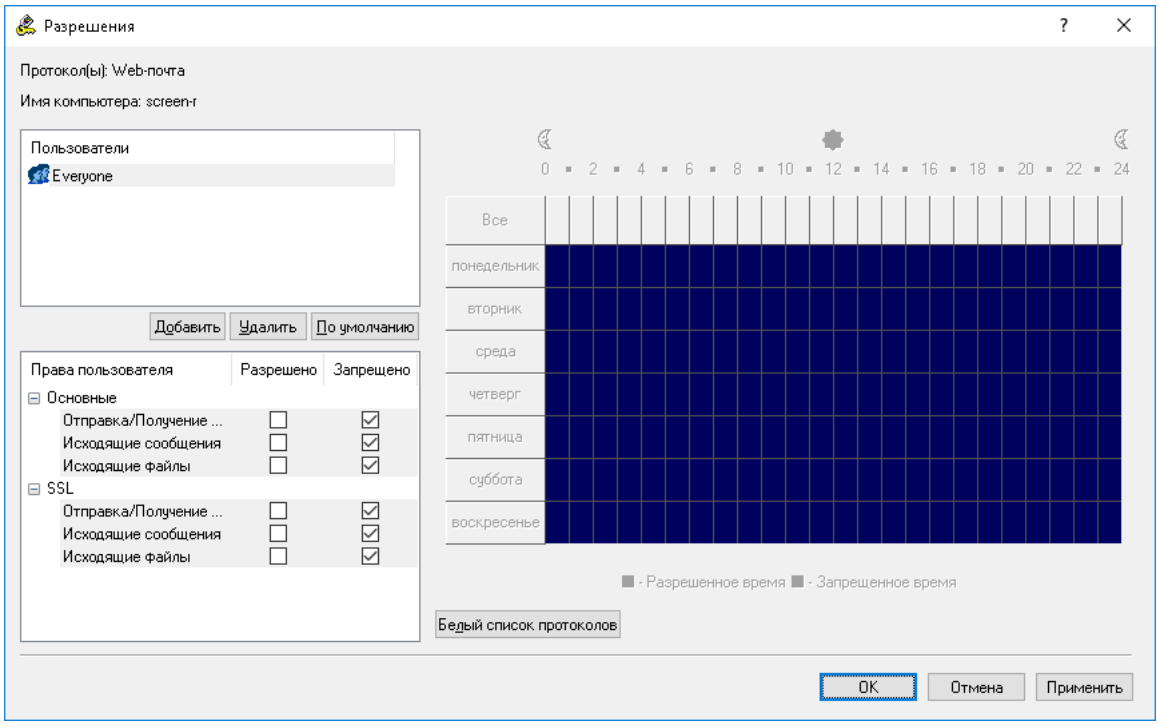


3. Нажмите **OK**, чтобы применить настройки и закрыть диалоговое окно **Аудит, Теневое копирование и Алерты**.

Примеры разрешений для протоколов

Для всех пользователей запрещена любая Web-почта, но Администраторы могут использовать Gmail:

1. В дереве консоли раскройте узлы **Сервис DeviceLock** -> **Протоколы**.
2. В узле **Протоколы** выберите **Разрешения**.
3. На панели сведений щелкните правой кнопкой мыши **Web-почта**, а затем выберите команду **Установить разрешения**.
4. В диалоговом окне **Разрешения** выполните следующие действия:
   a) В области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя учетной записи **Все**, а затем нажмите кнопку **OK**.
   b) В области **Пользователи** выберите запись **Все**.
   c) В области **Права пользователя** выберите **Запрещено** для всех прав.

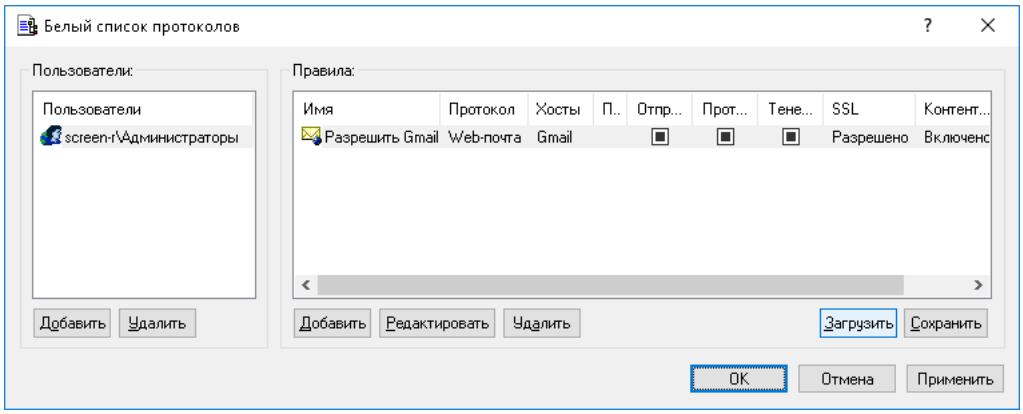


   d) Нажмите кнопку **Белый список протоколов**.

5. В диалоговом окне **Белый список протоколов** выполните следующие действия:

   a) В области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите **Администраторы**, а затем нажмите кнопку **OK**.

   b) В области **Пользователи** выберите запись **Администраторы**, а затем в области **Правила** нажмите кнопку **Добавить**. В диалоговом окне **Добавить правило** в поле **Имя** введите имя правила. Далее, в области **Сервисы Web-почты** установите флажок **Gmail**, а затем нажмите кнопку **OK**.



   c) Нажмите кнопку **OK** или **Применить**, чтобы применить настройки белого списка и закрыть диалоговое окно **Белый список протоколов**.

6. В диалоговом окне **Разрешения** нажмите кнопку **OK** или **Применить**.

Группе FileSharing Trusted Users разрешено использовать клиентские Windows-приложения Dropbox, Яндекс.Диск и Backup and Sync from Google (бывш. Google Drive Sync):

1. В дереве консоли раскройте узлы **Сервис DeviceLock** -> **Протоколы**.
2. В узле **Протоколы** щелкните правой кнопкой мыши **Белый список**, а затем выберите команду **Управление**.
3. В диалоговом окне **Белый список протоколов** выполните следующие действия:

   a) В области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя группы **FileSharing Trusted Users**, а затем нажмите кнопку **OK**.

   b) В области **Пользователи** выберите запись **FileSharing Trusted Users**, а затем в области **Правила** нажмите кнопку **Добавить**.

4. В диалоговом окне **Добавить правило** выполните следующие действия:

   a) В списке **Протокол** выберите **SSL**.

   b) В поле **Имя** введите имя правила.

c) В поле **Хосты** введите следующие имена серверов через запятую или точку запятой:

- Серверы Dropbox:

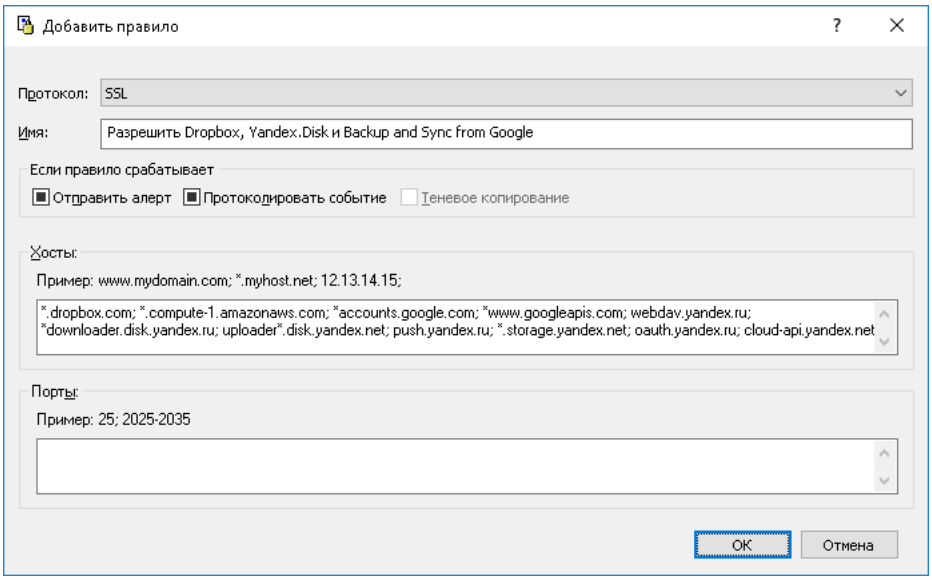
  `*.dropbox.com; *.compute-1.amazonaws.com`

- Серверы Google:

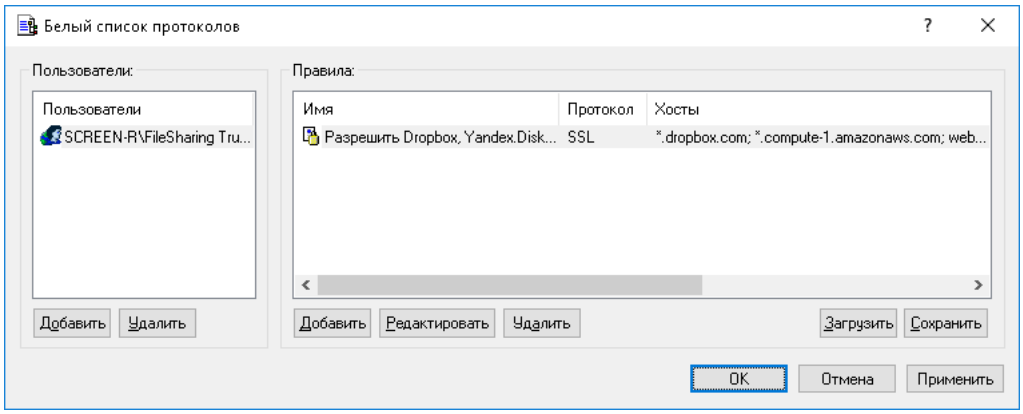
  `*accounts.google.com; *www.googleapis.com`

- Серверы Яндекс.Диск:

  `webdav.yandex.ru; *downloader.disk.yandex.ru; uploader*.disk.yandex.net; push.yandex.ru; *.storage.yandex.net; oauth.yandex.ru; cloud-api.yandex.net`



d) Нажмите кнопку **OK**.



5. Нажмите кнопку **OK** или **Применить**, чтобы применить настройки белого списка и закрыть диалоговое окно **Белый список протоколов**.

Примечание: Контроль доступа, аудит, теневое копирование и фильтрация содержимого будут отключены для всех сеансов передачи файлов.

Примеры контентно-зависимых правил

Всем пользователям запрещено копировать на устройства хранения (диски, съемные накопители) и передавать по сети (по протоколам HTTP, FTP, SMTP, Web-почта) следующие типы содержимого: файлы, содержащие номера кредитных карт; документы и архивы, защищенные паролем; файлы, содержащие номера социального обеспечения (US Social Security Number), а также изображения, содержащие большой объем текста.

1. В дереве консоли раскройте узел **Сервис DeviceLock**, раскройте узел **Устройства**, щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.
2. В диалоговом окне **Контентно-зависимые правила для устройств** в области **База данных контента** щелкните стрелку рядом с полем **Добавить группу**, а затем выберите пункт **Свойства документа**.
3. В диалоговом окне **Добавить группу свойств документа** выполните следующие действия:
   a) В поле **Имя** введите имя группы, например, **Защищенные паролем документы и архивы**.
   b) Установите флажок **Защищен паролем**.
   c) Нажмите кнопку **OK**.

   Созданная контентная группа добавляется в список существующих контентных групп в области "База данных контента" диалогового окна "Контентно-зависимые правила для устройств". Эта группа будет использоваться для контроля доступа к защищенным паролем документам и архивам.
4. В диалоговом окне **Контентно-зависимые правила для устройств** в области **База данных контента** щелкните стрелку рядом с полем **Добавить группу**, а затем выберите пункт **Свойства документа**.
5. В диалоговом окне **Добавить группу свойств документа** выполните следующие действия:
   a) В поле **Имя** введите имя группы, например, **Изображения, содержащие 70% текста**.
   b) Установите флажок **Содержит текст** и задайте значение **70%**.
   c) Нажмите кнопку **OK**.

   Созданная контентная группа добавляется в список существующих контентных групп в области "База данных контента" диалогового окна "Контентно-зависимые правила для устройств". Эта группа будет использоваться для контроля доступа к графическим изображениям с большим количеством текста.
6. В диалоговом окне **Контентно-зависимые правила для устройств** в области **База данных контента** щелкните стрелку рядом с полем **Добавить группу**, а затем выберите пункт **Составное**.

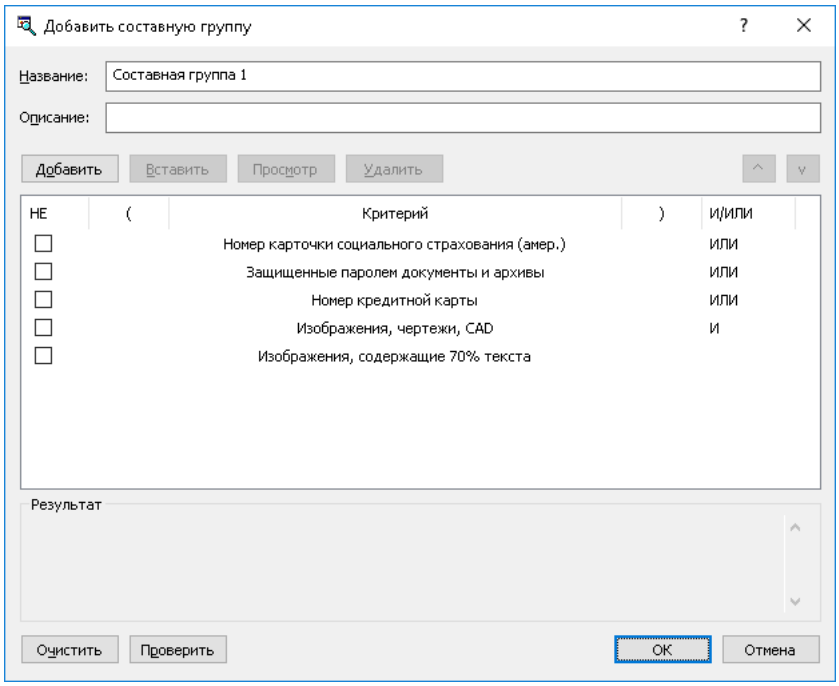
7. В диалоговом окне **Добавить составную группу** выполните следующие действия:

   a) В поле **Имя** введите имя группы, например, **Составная группа 1**.

   b) Нажмите кнопку **Добавить**. В диалоговом окне **Контентные группы** выберите следующие группы: **Защищенные паролем документы и архивы**; **Изображения, чертежи, CAD**; **Изображения, содержащие 70% текста**; **Номер карточки социального страхования (амер.)**; **Номер кредитной карты**.

   Можно выбрать эти группы одновременно, удерживая при нажатии клавишу CTRL.

   c) Составьте следующее логическое выражение: **Номер карточки социального страхования (амер.) ИЛИ Защищенные паролем документы и архивы, ИЛИ Номер кредитной карты ИЛИ Изображения, чертежи, CAD И Изображения, содержащие 70% текста**.



   d) Нажмите кнопку **OK**.

Созданная контентная группа добавляется в список существующих контентных групп в области "База данных контента" диалогового окна "Контентно-зависимые правила для устройств". Эта группа будет использоваться для контроля доступа к файлам, содержащим номера кредитных карт, защищенным паролем документам и архивам, файлам, содержащим номера социального обеспечения (US Social Security Number), и графическим изображениям с большим количеством текста.

8. В диалоговом окне **Контентно-зависимые правила для устройств** выполните следующие действия:

   a) В области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя учетной записи **Все**, а затем нажмите кнопку **OK**.

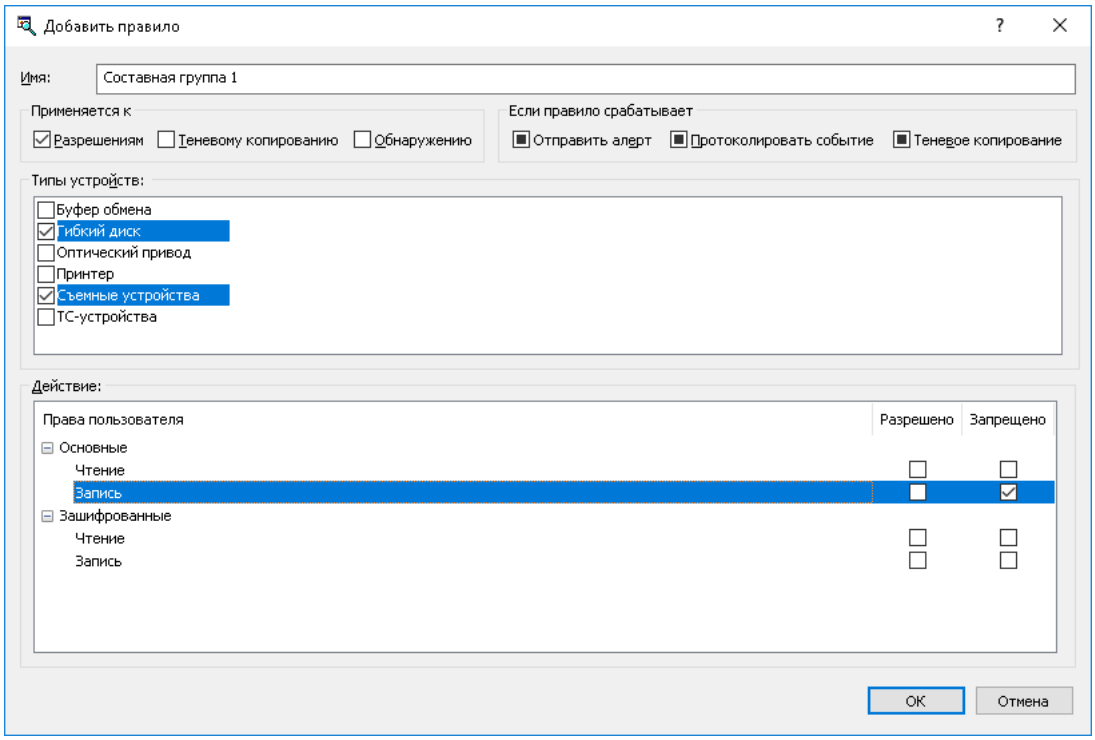
   b) В области **Пользователи** выберите запись **Все**. В области **База данных контента** выберите контентную группу **Составная группа 1**, а затем нажмите кнопку **Добавить**.

9. В диалоговом окне **Добавить правило** выполните следующие действия:

   a) В области **Применяется к** установите флажок **Разрешениям**.

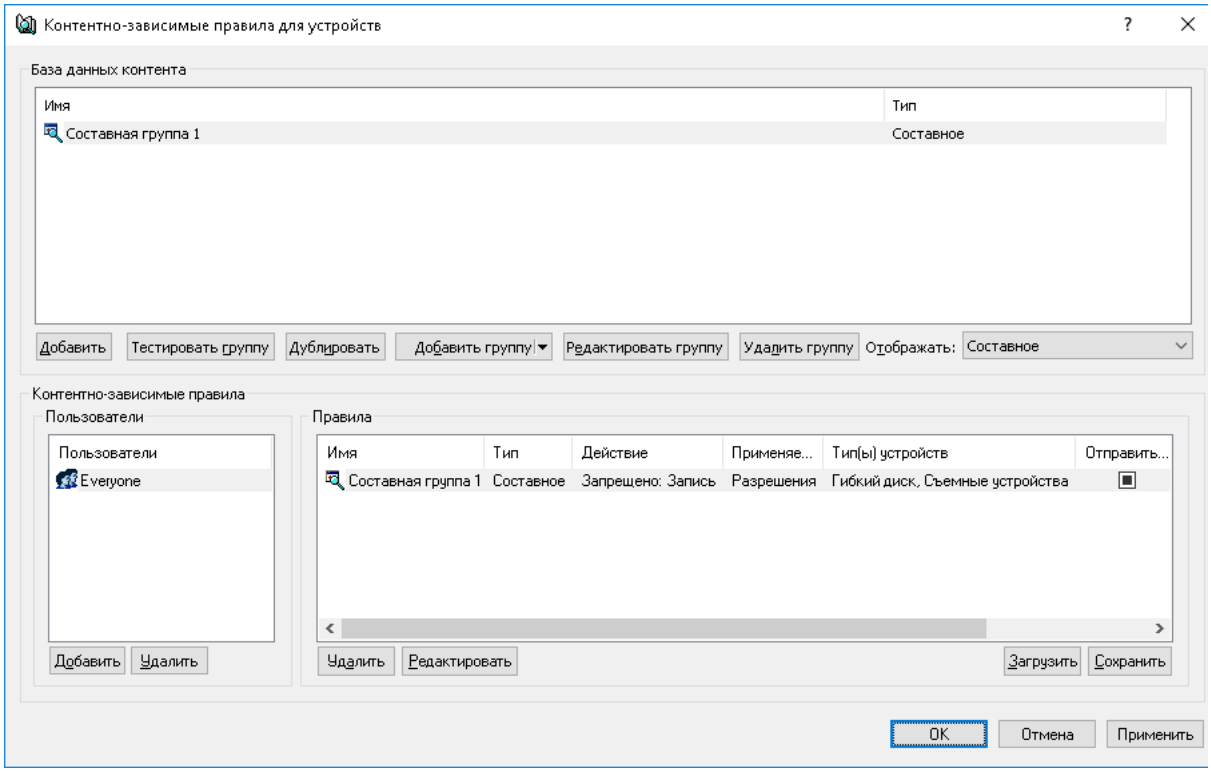
   b) В области **Типы устройств** установите флажки **Гибкий диск** и **Съемные устройства**.

   c) В области **Действие** установите флажок **Запрещено** для права **Запись**.



   d) Нажмите кнопку **OK**.

10. В диалоговом окне **Контентно-зависимые правила для устройств** нажмите кнопку **OK** или **Применить**, чтобы применить правило.



11. В дереве консоли раскройте узел **Протоколы**, щелкните правой кнопкой мыши **Контентно-зависимые правила**, а затем выберите команду **Управление**.

12. В диалоговом окне **Контентно-зависимые правила для протоколов** выполните следующие действия:

    a) В области **Пользователи** нажмите кнопку **Добавить**. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя учетной записи **Все**, а затем нажмите кнопку **OK**.

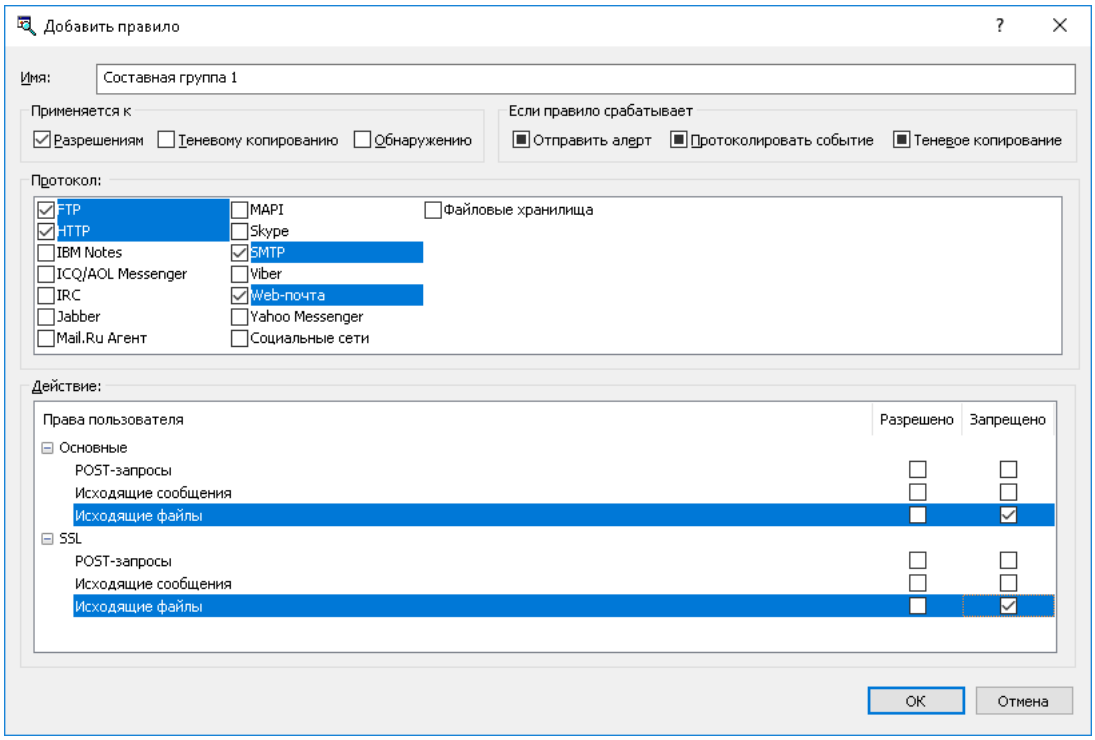
    b) В области **Пользователи** выберите запись **Все**. В области **База данных конткнта** выберите контентную группу **Составная группа 1**, а затем нажмите кнопку **Добавить**.

13. В диалоговом окне **Добавить правило** выполните следующие действия:

a) В области **Применяется к** установите флажок **Разрешениям**.

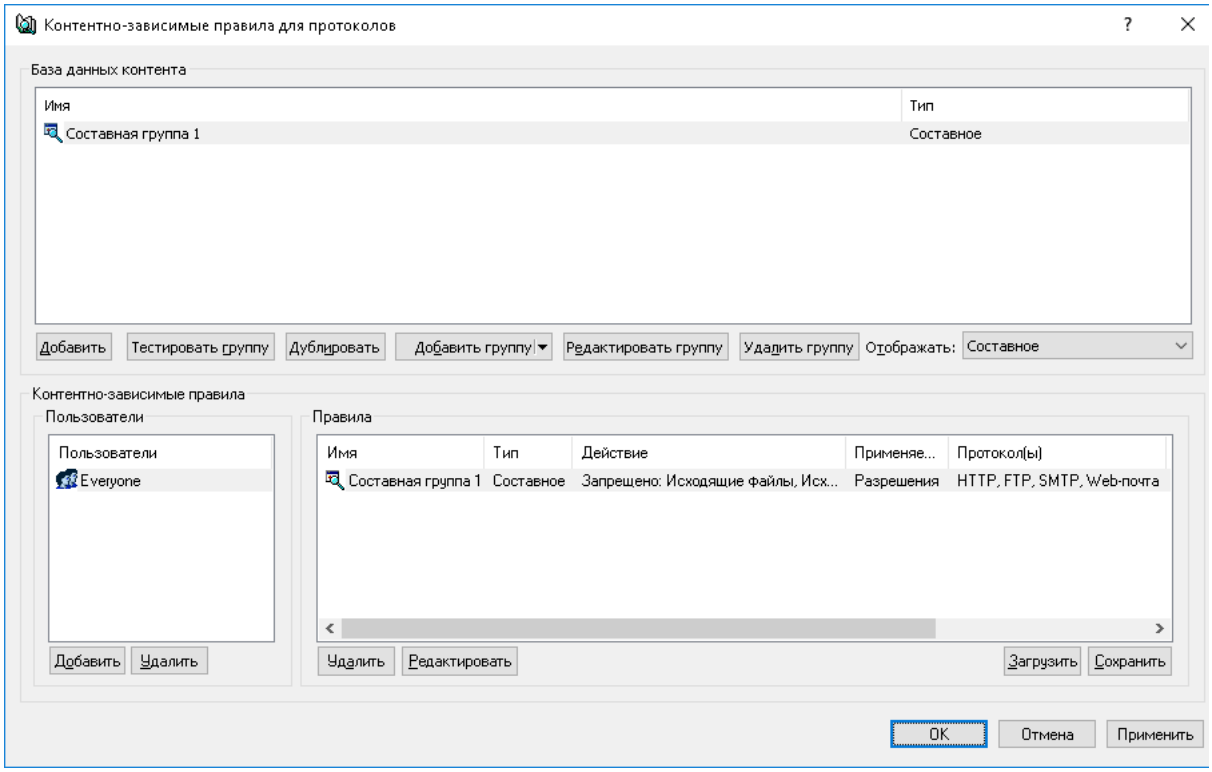
b) В области **Протокол** установите флажки **FTP**, **HTTP**, **SMTP** и **Web-почта**.

c) В области **Действие** установите флажок **Запрещено** для следующих прав: **Основные: Исходящие файлы** и **SSL: Исходящие файлы**.



d) Нажмите кнопку **OK**.

14. В диалоговом окне **Контентно-зависимые правила для протоколов** нажмите кнопку **OK** или **Применить**, чтобы применить правило.



Примеры правил IP-файрвола

Ниже показаны примеры правил, которые можно создать для IP-файрвола.

IP-файрвол блокирует подключения к удаленному рабочему столу на компьютерах с работающим сервисом DeviceLock:

1. В дереве консоли раскройте узлы **Сервис DeviceLock** -> **Протоколы**.
2. В узле **Протоколы** щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление**.
3. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** нажмите кнопку **Добавить**.
4. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя учетной записи **SYSTEM**, а затем нажмите кнопку **OK**.
5. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** выберите запись **SYSTEM**.
6. В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** нажмите кнопку **Добавить**.
7. В диалоговом окне **Добавить правило** выполните следующие действия:
   a) В поле **Имя** введите имя правила файрвола, например **Закрыть доступ к RDP**.
   b) В области **Протокол** установите флажки **TCP** и **UDP**.
   c) В области **Тип** выберите **Запрет**.
   d) В области **Направление** установите флажок **Входящие**.
   e) В поле **Порты** введите `3389`.
   f) Нажмите кнопку **OK**.
8. Нажмите кнопку **OK** или **Применить**, чтобы применить настройки правила файрвола и закрыть диалоговое окно **Базовый IP-файрвол**.

Файрвол разрешает входящие подключения по протоколу POP3 для указанного пользователя, блокируя любые другие подключения к компьютеру с работающим сервисом DeviceLock:

1. В дереве консоли раскройте узлы **Сервис DeviceLock** -> **Протоколы**.
2. В узле **Протоколы** щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление**.
3. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** нажмите кнопку **Добавить**.
4. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя учетной записи **Все**, а затем нажмите кнопку **OK**.
5. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** выберите запись **Все**.
6. В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** нажмите кнопку **Добавить**.
7. В диалоговом окне **Добавить правило** выполните следующие действия:
   a) В поле **Имя** введите имя правила файрвола, например **Закрыть доступ**.
   b) В области **Протокол** установите флажки **TCP** и **UDP**.
   c) В области **Тип** выберите **Запрет**.
   d) В области **Направление** установите флажок **Входящие**.
   e) В поле **Порты** введите `0-65535`.
   f) Нажмите кнопку **OK**.

   Созданное правило появится в области "Правила" в правой части диалогового окна "Базовый IP-файрвол". Это правило будет использоваться для блокирования всех удаленных подключений к клиентскому компьютеру.
8. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** нажмите кнопку **Добавить**.
9. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя пользователя или группы, которым разрешено использовать POP3, а затем нажмите кнопку **OK**.
10. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** выберите пользователя или группу, которым разрешено использовать протокол POP3.
11. В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** нажмите кнопку **Добавить**.
12. В диалоговом окне **Добавить правило** выполните следующие действия:
    a) В поле **Имя** введите имя правила файрвола, например **Открыть доступ к POP3**.
    b) В области **Протокол** установите флажок **TCP**.
    c) В области **Тип** выберите **Разрешение**.
    d) В области **Направление** установите флажок **Входящие**.
    e) В поле **Порты** введите `110`.
    f) Нажмите кнопку **OK**.

    Созданное правило появится в области "Правила" в правой части диалогового окна "Базовый IP-файрвол". Это правило будет использоваться для разблокирования в файрволе порта 110, чтобы пользователь мог создавать подключения по протоколу POP3.
13. Нажмите кнопку **OK** или **Применить**, чтобы применить настройки правила файрвола и закрыть диалоговое окно **Базовый IP-файрвол**.

Файрвол запрещает все входящие и исходящие TeamViewer-соединения с компьютером, на котором работает сервис DeviceLock:

1. В дереве консоли раскройте узлы **Сервис DeviceLock** -> **Протоколы**.
2. В узле **Протоколы** щелкните правой кнопкой мыши **Базовый IP-файрвол**, а затем выберите команду **Управление**.
3. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** нажмите кнопку **Добавить**.
4. В диалоговом окне **Выбор: "Пользователи" или "Группы"** в поле **Введите имена выбираемых объектов** введите имя учетной записи **Все**, а затем нажмите кнопку **OK**.
5. В левой части диалогового окна **Базовый IP-файрвол** в области **Пользователи** выберите запись **Все**.
6. В правой части диалогового окна **Базовый IP-файрвол** в области **Правила** нажмите кнопку **Добавить**.
7. В диалоговом окне **Добавить правило** выполните следующие действия:
   a) В поле **Имя** введите имя правила файрвола, например **Закрыть доступ к TeamViewer**.
   b) В области **Протокол** установите флажок **TCP**.
   c) В области **Тип** выберите **Запрет**.
   d) В области **Направление** установите флажок **Исходящие**.
   e) В поле **Порты** введите **5938**.
   f) Нажмите кнопку **OK**.

   Созданное правило появится в области "Правила" в правой части диалогового окна "Базовый IP-файрвол". Это правило будет использоваться для блокирования всех подключений к серверам TeamViewer.
8. Нажмите кнопку **OK** или **Применить**, чтобы применить настройки правила файрвола и закрыть диалоговое окно **Базовый IP-файрвол**.