

Detection and Response

Table of contents

Product Overview	9
About Detection and Response	9
The Detection and Response Approach and Solution Architecture	9
System Architecture and Components	10
System Requirements	11
Detection and Response's Behavior Pattern Mapping	11
Detection and Response's Protection Modules	12
Terms and Concepts	13
System Components	13
Security Concepts	14
Assets and Their Properties	15
Analyzing Events	15
Handling Events	16
Accessing the Detection and Response Management Environment	16
Detection and Response Monitoring Environment Console Overview	17
Viewing Server Information	18
Configuring Server Time Zone	19
Working with the Detection and Response Monitoring Environment Dashboard	21
Detection and Response Monitoring Environment Dashboard Overview	21
Dashboard Interface	21
Selecting a Dashboard Timeframe	22
Understanding the Detection and Response Monitoring Environment Dashboard Summary View	24
Infected Endpoints Summary	24
Malicious Processes Summary	25
Drilling Down to Detailed Dashboard Data	26
How to Drill Down	27
Viewing Malware Information	29
Viewing Activity Data	31
Handling Events in the Dashboard View	33
Exporting Dashboard Data	35
Clearing Data from the Dashboard	35
Adding an Exception from the Detection and Response Monitoring Environment Dashboard	37
Using the Detection and Response Management Console Security Center	40
The Security Center: Overview	40
Accessing the Security Center	40

Filtering the Display	41
Security Center Home Screen	43
Security Snapshot Panel	44
Asset Vulnerability Overview	45
Detection and Response Management Console Security Center: Initial Drilldown	50
Malicious Process Drilldown	50
Attacked Asset Drilldown	51
Security Center Full Drilldown: Analyzing Incident Forensics	51
Incident Forensics: Display Options	53
The Event Forensic Storyline	54
Handling Endpoints in the Detection and Response Monitoring Environment	56
Endpoint Management Overview	56
Viewing the Endpoints List	56
Understanding the Endpoints Grid	57
Viewing Detailed Endpoint Information	58
Filtering the Endpoints List	59
Performing Actions on Endpoints	62
Managing Static Group Assignments	64
Working with the Manage Group Assignments Dialog	64
Managing Group Assignments: Use Case Example	66
Defining Default Endpoint Settings	68
Setting Agent and BPM Default Versions	69
Selecting Endpoint Global Settings	70
Configuring Advanced Agent Settings	72
Accessing Advanced Agent Settings	72
Selecting Settings for the Armed Agent	74
Specifying Trusted Applications	75
Accessing Trusted Applications Settings	75
Selecting the Trusted Applications Level	77
Building and Maintaining the Trusted Applications List	78
Using the Remote Mode-Switching (RMS) Tool	79
Setting Up the RMS Tool	79
Running the RMS Tool	80
Alternatives to Command-line Parameters	81
RMS Tool Exit Codes	82
More About the RMS Tool	82
Handling Assets in the Detection and Response Management Console	83

Viewing the Assets List	83
Understanding the Assets Grid	83
Filtering the Assets List	85
Performing Actions on Assets	87
Quarantine Asset	87
Save Selected Asset List	88
Managing Endpoint Groups	90
Endpoint Groups: Overview	90
Understanding the Groups Tab	90
Assigning Group Priority	91
Adding and Deleting Groups	92
Creating an Endpoints Group	93
Deleting Groups	94
Configuring Settings for Groups	95
Updating Group Name and Details	96
Maintaining Group Endpoints	97
Selecting Update Versions	98
Selecting Agent Behavior Settings and Update Rules	98
Assigning Endpoints to Groups	100
Managing Static Group Assignments	100
Configuring Auto Assign Rules for Dynamic Groups	101
Controlling Network Usage	102
Total Downstream Bandwidth Management	102
Group Bandwidth Management	103
Analyzing Processes in the Detection and Response Monitoring Environment	105
Viewing Processes in the Detection and Response Monitoring Environment	105
Viewing Process Details	106
Viewing Potential Process Interruptions	106
Understanding the Detection and Response Monitoring Environment Processes Tab	107
Filtering the Detection and Response Monitoring Environment Processes List	109
Analyzing Processes in the Detection and Response Management Console	111
Viewing Processes in the Detection and Response Management Console	111
Understanding the Detection and Response Management Console Processes Grid	112
Managing Processes in the Detection and Response Management Console	113
Block Process	113
Export	114

Viewing and Managing Exceptions in the Detection and Response Monitoring Environment	115
Policies Overview	115
Understanding the Policies Tab	115
Adding a Policy from the Policies Tab	117
Managing Policies in the Detection and Response Monitoring Environment	119
Exporting and Importing Policies	120
Disabling and Enabling Policies	121
Updating Policies	122
Managing Matching Activities	123
Deleting Policies	125
Creating and Maintaining the Default Policy Set	126
Maintaining the Default Policy Set	128
Applying Policies to Endpoint Groups	129
Maintaining Group Policies	130
Configuring Automatic Exception Retirement	130
Viewing and Managing Exceptions in the Detection and Response Management Console	132
Working with the Exceptions Menu	132
Understanding the Exceptions Grid	133
Adding Exceptions in the Detection and Response Management Console	134
Exception Management in the Detection and Response Management Console	138
Disabling and Enabling Exceptions	139
Deleting Exceptions	139
Handling Matching Activities	140
Working with Hardening Policies	143
Hardening Policies: Overview	143
Defining Hardening Policies in the Detection and Response Management Console	143
Working with the Hardening Policies Set	144
Accessing the HP Page	144
Viewing and Managing the Hardening Policies List	145
Understanding Hardening Policy Parameters	148
Use Case Summary	148
Initiator and Target Parameters	148
Adding Hardening Policies to Your HP Set	151
Importing Hardening Policies	151
General Guidelines for Creating and Updating Hardening Policies	152
Specifying HP General Parameters	154

Assigning Hardening Policies to Groups	156
Handling Administrative Operations	159
Viewing Detection and Response Monitoring Environment Reports	159
Assets Overview	160
Assets by Threat	161
Attacks by Hour/Day	162
Prevented Processes	164
Detection and Response Monitoring Environment User Activity	165
Managing Users	165
Adding New Users	167
Updating User Details	168
Handling Update Packages	171
Uploading Update Packages	172
Managing Agent and BPM Versions	173
Defining License Approval Settings	175
Viewing User Records in the Logs Tab	176
Filtering the Log Records	177
Deleting Log Records	179
Managing Detection and Response from an Endpoint	180
Viewing Events History	181
Viewing Selected Detection and Response Settings	181
Performing Server Administration	183
Server Management Operations	183
Configuring Endpoint Pinging Capability	184
Configuring SIEM Integration	185
Specifying SIEM Integration Settings	185
Understanding Events Log Information	188
Understanding the Identified Threats Report	193
Understanding Detection and Response Monitoring Environment Log Information	195
Configuring SAML Integration	196
Viewing and Downloading Log Files	198
Retrieving a Single Log File	199
Handling Agent Offline Installation	199
Agent Version Considerations	200
Managing Server Storage	202
Configuring Cleanup Alert Settings	203
Performing Server Cleanup	203

Handling Database Files	206
Managing the Database List	206
Performing Database Backup	209
Clearing the Database	210
Caution	210
Viewing Database Logs	211
Index	213

Copyright statement

© Acronis International GmbH, 2003-2021. All rights reserved.

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

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

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

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

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

Acronis patented technologies

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

Product Overview

About Detection and Response

Detection and Response is a comprehensive cyber security solution that monitors system events on end user workstations and identifies possible threats to the system. The technology used to detect potential security attacks is based on detailed analysis of the operating system behaviors (activities) taking place at the workstation's kernel level.

The Behavioral Patterns Map (BPM) is a unique analysis technique that categorizes all normal behaviors of the operating system into sets of predefined behavior patterns. Any unauthorized method of performing these behaviors (e.g., deleting a file using a hidden command line) is identified as a deviant and potentially malicious operation. The BPM technique enables the analysis to be performed accurately and efficiently, without affecting user experience or workstation performance.

Once the Detection and Response system is installed and configured, the Detection and Response Monitoring Environment management tool provides administrators with full visibility and control of processes and behavior occurring on endpoints. Any unauthorized or potentially hazardous activity or process in an endpoint can thus be quickly identified and handled. In addition, administrators can use the Detection and Response Monitoring Environment to define security policies, generate reports, and perform other management activities.

This guide explains the main functions and capabilities of the Detection and Response Monitoring Environment, and provides administrative users with a quick reference to commonly performed procedures and management tasks.

The Detection and Response Approach and Solution Architecture

Acronis Detection and Response is a threat-agnostic endpoint and server security solution designed to detect and prevent unknown-unknown threats. Detection and Response prevents targeted APT, zero-day and other highly sophisticated cyber attacks, regardless of whether any prior knowledge about the threat exists.

Detection and Response is the world's first threat-agnostic defense solution that can identify and stop a new attack without the need for any breadcrumbs, baseline or other prior knowledge. This all new approach to stopping attacks is based on mapping operating systems at the kernel and system call level with exacting cartography. Instead of analyzing vector points, attack methodologies and comparing malware spread mechanisms whose numbers can reach multi billions per year, Detection and Response focuses on the most common denominator of all threats - the damage.

The Detection and Response approach leverages a patented way of mapping out all normative ways to perform actions on a desktop or server. A user can delete, exfiltrate, manipulate, or encrypt data in just a few simple clicks during the course of normal work. However in the background, at the

kernel level of the operating system, these few mouse clicks can represent dozens of thousands of system calls to the operating system. Acronis Detection and Response is specifically designed to map and track all these operating system calls and verify that they adhere to strictly normative methodologies that are consistent with legitimate use. This approach has been proven to successfully improve malware detection and prevent damage to assets.

System Architecture and Components

The solution architecture includes the following main components:

- **LT:** A Detection and Response Tray utility that displays information about Agent and BPM configurations. It can also show the history of denied events detected by Detection and Response on an endpoint.
- **PS Tool:** This utility runs in the user space. It collects information about running applications and passes the data to the Driver. The BPM Engine in the Driver uses the information provided by the PS Tool for analysis.
- **Detection and Response Agent:** The Agent is a Windows Service that gets information from the Driver (e.g., events detected and statistical data) and sends it to the Detection and Response Backend System. The Agent also receives system configuration data, such as new BPM Policies, from the Backend System.

The protection level of the Detection and Response Agent can be set to either Prevention mode, to block threats, or Detection mode, to report threats to the Backend System. Even when an Agent is not connected to the server backend, Detection and Response continues to run and to protect the device.

- **Detection and Response License Installer:** A standalone application for initial installation of the Detection and Response Agent. This application communicates with the Backend System to obtain the Detection and Response Agent installer, licenses, configuration, BPM rules and more.
- **Detection and Response Minifilter Driver:** A Windows Driver that registers system callbacks, hooks and events for monitoring. Detection and Response monitors every important system call, including file, registry, process and network operations.

The Driver contains a module called the Behavior Pattern Mapping (BPM) Engine. For more information, refer to the sections below.

- **Detection and Response Backend System:** Also known as the Detection and Response Server, this component receives events and statistical information from endpoints, and stores this information in the database. The Backend System provides administrators with UI access to the system via the Detection and Response Management Environment. The Detection and Response Monitoring Environment displays detailed data about system settings, detected threats, and other endpoint security information. It also enables authorized users to manage security settings, upgrade BPM and Agent versions, investigate attacks, and more. The Server can be deployed as a physical appliance, as a VM, or in the Cloud.

System Requirements

Minimum system requirements

- Hardware:
 - Processor: Intel Core 2 duo, 2GHz or equivalent
 - Memory: 4GB
- Software:
 - Framework: .NET 2.0
 - SHA256 support
 - Storage: 1.1GB of available space (installation 100MB, maintenance 1GB)

Supported operating systems

Detection and Response can run on the following operating systems:

- Workstations:
 - Windows 7 (32-bit and 64-bit)
 - Windows 10 (64-bit)
- Servers:
 - Windows Server 2008 R2 (64-bit)
 - Windows Server 2012 R2 (64-bit)
 - Windows Server 2016 (64-bit)
 - Windows Server 2019 (64-bit)

Detection and Response's Behavior Pattern Mapping

Based on a new, proprietary programming language developed by Acronis, the patented BPM is the first-ever language developed specifically to map legitimate complexed OS behaviors. Using the BPM, Detection and Response is capable of analyzing hundreds of thousands of system calls in real time. The unique Operating System research and maintenance of the BPM is conducted by Acronis Security Research Team experts.

The BPM's main advantage is that it makes Detection and Response a threat-agnostic solution which renders the attack vector irrelevant. Malware will be blocked on its first attempt to cause damage, regardless of where it came from. Whether the attack method includes a USB flash-drive, a remote/local exploit, a file-less approach or some other attack vector, Detection and Response will be able to detect and prevent the attack without any prior knowledge or attack-related research. Hence, while attackers focus on developing new sophisticated techniques, these remain irrelevant to Detection and Response.

Since Detection and Response's methodology is purely deterministic, it can even detect threats that already exist in the system. Although Detection and Response does not scan for the presence of

signatures on an endpoint upon first deployment, there is no impact on detection abilities. Detection and Response will prevent any damage from occurring as soon as the threat becomes active.

Here are just a couple of examples showing how the BPM approach effectively prevents damage:

- Detection and Response will block actions such as process injection, persistency-establishing activity (e.g., registry entry creation under Run or RunOnce) and a malicious attempt to communicate with an external server. Each of these actions is identified by a set of specific system calls that may be in the order of hundreds of thousands of unique calls. However, since the sequence of actions /system calls does not match any of the normative paths defined by BPM, they will not be allowed.
- Detection and Response's approach to threat detection will prevent ransomware damage. The BPM has a map of all normative ways to delete or override a file, and defines rules accordingly. Any other method of file handling is considered to be malicious, and Detection and Response will block it.

Note

Detection and Response is integrated with the Windows Defender Security Center. When the Security Center detects the Detection and Response Agent, it automatically disables its own active anti-virus functionality. If desired, you may still schedule periodic scans to be run by Windows Defender.

Detection and Response's Protection Modules

The BPM (Behavioral Patterns Mapping) analysis method used by the Detection and Response Agent categorizes all behaviors taking place on the endpoint into Protection Modules. The Protection Modules protect essential data and resources by detecting specific behaviors that may be hazardous or malicious.

Each Protection Module safeguards the endpoint from a specific type of threat. The different Protection Modules and their functions are described in the following table.

Protection Module Name	Description
Abnormal Communication	Protects against malicious network communication.
Application Tampering	Protects against malicious modification of installed applications.
Browser Hijacking	Protects browser settings from harmful modifications.
Code Injection	Protects against malicious code injection.
Data Corruption	Protects various types of valuable data, such as media, documents and archives, from being corrupted or manipulated.

Protection Module Name	Description
Evasion	Protects against elusive mechanisms of malware.
Local Data Exfiltration	Protects against data theft using removable storage.
Partition Corruption	Protects disk partitions from being altered.
Persistence	Protects sensitive persistence areas.
Registry Manipulation	Protects sensitive registry keys from malicious modifications.
Shell Access	Protects against execution of an illegitimate command line shell.
Shell Activity	Protects against illegitimate shell executions.
System File Impairment	Protects critical Windows system files.
System Security Alteration	Protects against illicit modification of system security settings.
Unauthorized Access Request	Protects processes and threads from being accessed illegitimately.

Terms and Concepts

The following tables provide definitions for terms and concepts commonly encountered while working with Detection and Response.

System Components

Term / Concept	Definition
Agent/BPM package	A compressed file containing updates for the Agent and/or BPM.
Asset	A workstation or server on which the Detection and Response Agent is installed.
Endpoint	A workstation on which the Detection and Response Agent is installed.
Detection and Response Server	A server dedicated to collecting the results of the Agents' behavioral analysis and storing this information in a dedicated database.
PM	Protection Module: A category of protection provided by the Detection and Response Agent. Each PM safeguards Assets from a specific type of threat.
Detection and Response Management Console	Detection and Response Management Console: A web-based administrative tool that provides advanced event analysis, Hardening Policy configuration capabilities and more.

Term / Concept	Definition
Detection and Response Monitoring Environment	Detection and Response Management Environment: A web-based dashboard that enables IT or security administrators to manage the Asset layer.
Server	A server on which the Detection and Response Agent is installed.
Server package	A compressed file containing updates for the Detection and Response Server.
WR	War Room: An optional premium management console that enables first responders to view the security status of all Assets in the organization.

Security Concepts

Term / Concept	Definition
Attacked Asset	An workstation or server on which a potentially malicious process has been identified.
BPM	Behavior Pattern Mapping: An analysis method that maps all normative operating system (OS) call flows. The Detection and Response Agent then thwarts non-normative system calls before their execution.
Compromised process	.
Detect	Identify the presence of potentially malicious processes.
Event	An occurrence in which a malicious process performed or attempted to perform one or more activities on an Asset. Events can be of critical, high, medium or low severity.
Intelligence	Information derived from external sources.
Malicious process	A running program that has the potential to compromise or damage the security of an Asset, and possibly result in a chain of events involving other processes and malicious activities.
Prevent	Block activities launched by potentially malicious processes.
Signature	A means of guaranteeing the authenticity of an electronic document.
Tainted process	A process that became compromised as a result of an operation performed by a malicious process.
Trusted Source	A file that is considered to be free of security threats, based on information gathered from cloud intelligence.
VirusTotal (VT)	A service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content.

Assets and Their Properties

Term / Concept	Definition
Group	A user-defined collection of Assets that usually have one or more common characteristics (e.g., location, department, etc.). Assets in a Group operate according to their own settings regarding Exception assignments, update rules, and more.
Hostname	A label assigned to a device connected to a computer network. This label is used to identify the device in various forms of electronic communication.
IP	A unique string of numbers, separated by periods, that identifies a computer using the Internet Protocol to communicate over a network.
OS	System software that manages the hardware and software resources of the computer, and provides common services for computer programs.
Pending	A Status in which an Asset has been sent an update by the Detection and Response Server.
Risk level (Group)	The degree of potential consequences in the event of a cyber attack on Assets in the Group. Risk level (High, Medium or Low) is assigned by the Administrator based on the value of the Group's Assets.
Status	The current state of Asset authorization in relation to the Detection and Response Server. An Approved Asset has a license to run and complies with Server policies.

Analyzing Events

Term / Concept	Definition
Caller	A process that attempted or performed a malicious operation.
Event forensics	A view in the Detection and Response Management Console Dashboard full drilldown that lists all activities generated on an Asset by a malicious process. Selecting an activity displays full details about that activity, including a Storyline visualization that lets the viewer easily see the flow of events involved.
Event time	The date and exact time at which a process performed or attempted to perform one or more activities on an Asset.
Hash	An identifier based on the MD5 (message digest) algorithm.
Parent process	The process that created the caller process.
Path	The file system location (e.g., of a process).
Publisher	The company or organization that digitally signed a process.

Term / Concept	Definition
Root cause	The source from which an attack originated, such as an e-mail client or a Web browser.
Session username	The user who was logged in during an event.
Status	Current handling status of an event, e.g., reviewed by a Security Analyst, confirmed to be malware, etc.
Target	The intended destination or file of a malicious process.

Handling Events

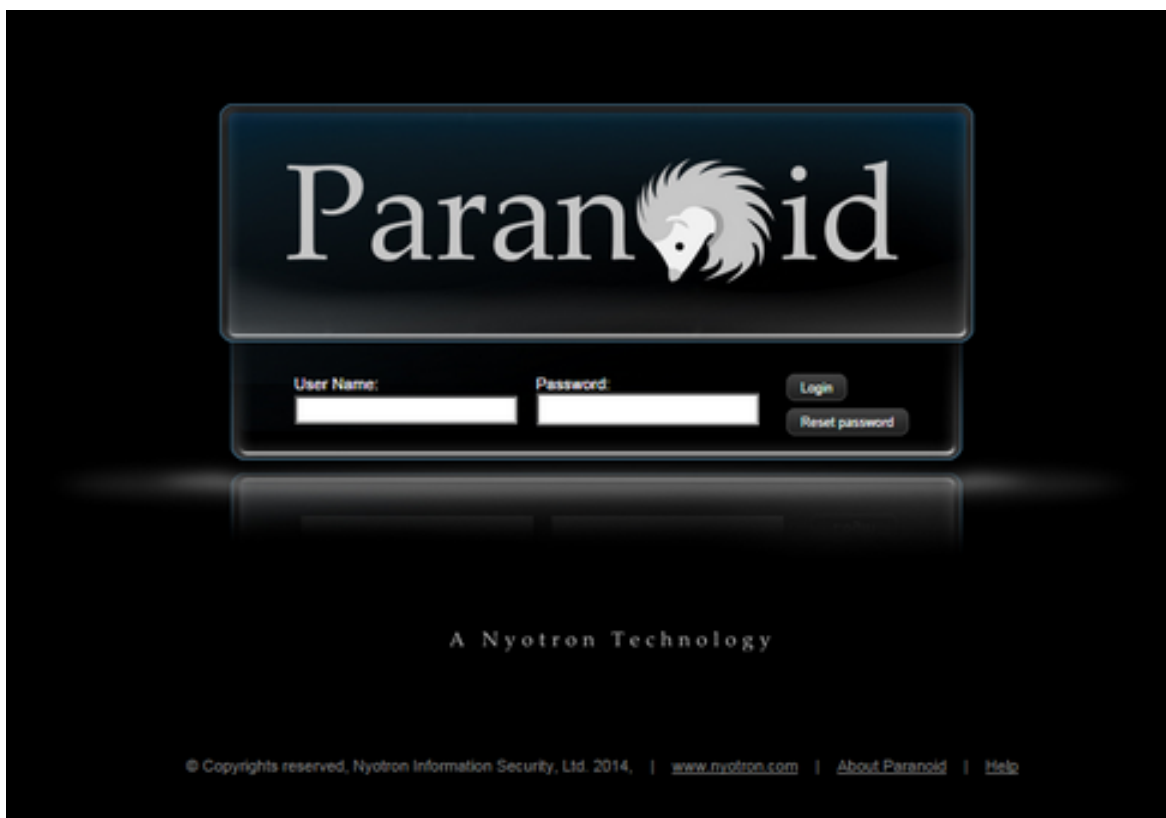
Term / Concept	Definition
Exception (Policy)	A rule that instructs the Agent to permit an action that it would normally block.
Hardening Policy	A user-defined rule that instructs the Agent to block or alert on an operation that would normally be allowed.

Accessing the Detection and Response Management Environment

Logging into the Detection and Response Monitoring Environment involves accessing the **Login** page and providing your administrative credentials.

To log in:

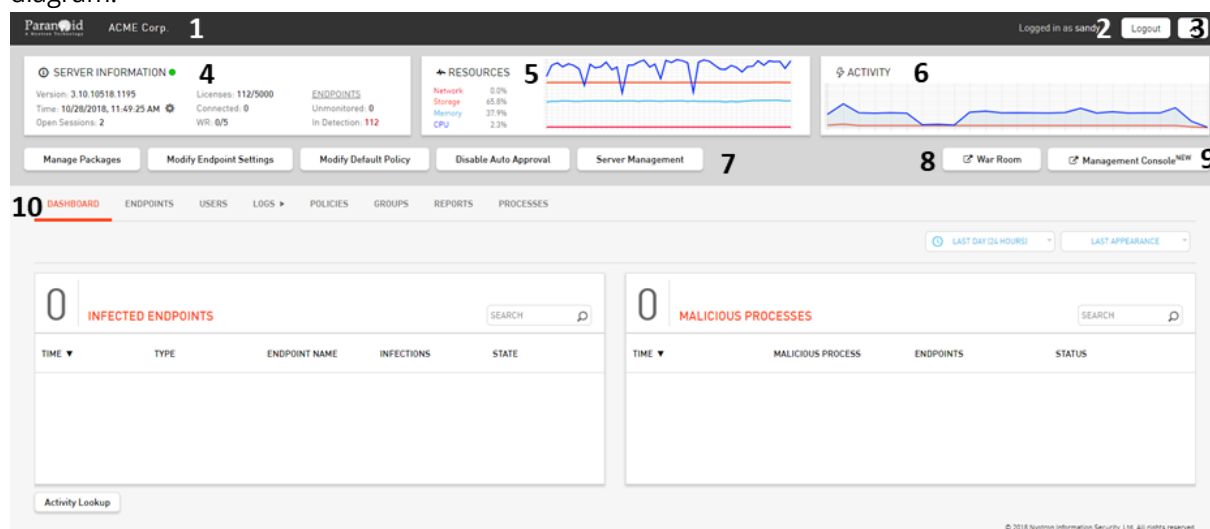
1. From your browser, access the **Login** page by entering the IP address of the Detection and Response Server.



2. Enter your user name and password in the appropriate fields, and then click **Login**.
The [Detection and Response Monitoring Environment console](#) opens, with the [Dashboard view](#) displayed by default.

Detection and Response Monitoring Environment Console Overview

Following a successful login, the Detection and Response Monitoring Environment console is displayed. The main components of the console are listed and described in the table below the diagram.

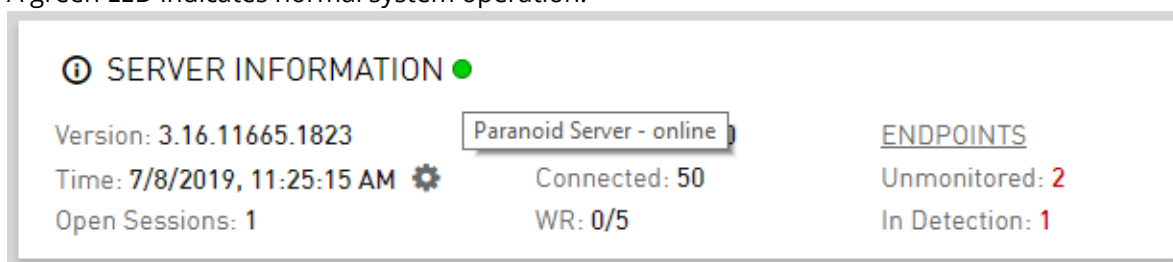


Number	Feature	Description
1	Customer title	Displays the name of your company.
2	Logout button	Ends your Detection and Response Monitoring Environment session, and redirects you to the Login page.
3	Show/Hide toggle	Use this toggle to show and hide the Server Information , Resources and Activity panes below.
4	Server Information	Displays general information about the Detection and Response Server and the current protection level of the endpoints. For details, refer to Viewing Server Information .
5	Resources	Displays information about current Detection and Response server resources (amount of consumed CPU, memory and storage).
6	Activity graph	Displays the number of malicious behaviors detected relative to all behaviors that were monitored in your set of endpoints.
7	Administrative action buttons	Enable you to perform specific management actions, such as sending updates, configuring endpoint settings, and updating policies.
9	Management Console button	Opens the Detection and Response Management Console, a new interface from which you can view events in an enhanced Security Center , create and manage your Hardening Policies set, and more.
10	System management tabs	Provide different views that allow you to manage the Detection and Response environment. Some of the options include managing the list of detected malicious processes, creating policies that define how to handle specific behaviors, monitoring Detection and Response Monitoring Environment user activity, and generating reports.

Viewing Server Information

This pane displays general server information, such as the version and the number of current open sessions. The color and appearance of the LED indicator at the top of the pane reflect the current connection status of the Server as well as the status of other system components and resources. Hovering over the LED opens a tooltip that describes the status and provides recommendations (if relevant).

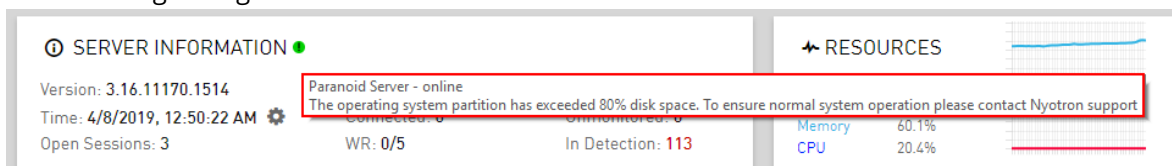
A green LED indicates normal system operation.



- A red LED indicates that the Server is offline.

A green LED with an exclamation mark indicates that the Server connection is normal, but that other components (license server and/or cloud intelligence) are offline. It can also indicate that

- Server storage is high.

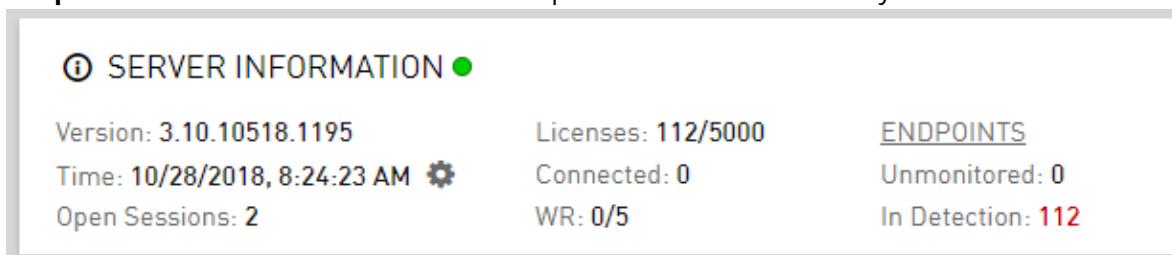


- An orange LED with an exclamation mark indicates that Server storage is approaching maximum capacity.

The **Server Information** pane also provides the following details:

- **Time:** The current date and time (according to the local time zone of the server). Users with advanced permissions (e.g., Root users) are able to change the time zone of the server. For details, refer to [Configuring Server Time Zone](#).
- **Licenses:** The number of licenses in use relative to the total number of available licenses.
- **WR:** The number of War Room licenses in use relative to the total number of available licenses.
- **Connected:** The number of endpoints that are currently connected to the Server.
- **Unmonitored Endpoints:** The number of endpoints that are not being monitored by the Agent, due to the current configuration of [advanced Agent settings](#).

Endpoints In Detection: The number of endpoints that are not currently in Prevention mode.



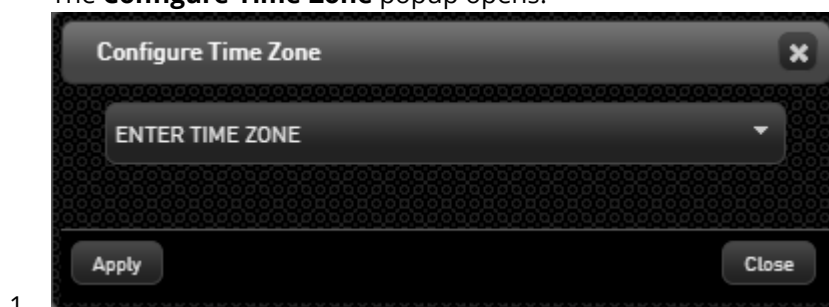
Configuring Server Time Zone

Follow the procedure below to change the time zone of the server.

To update the time zone of the server:

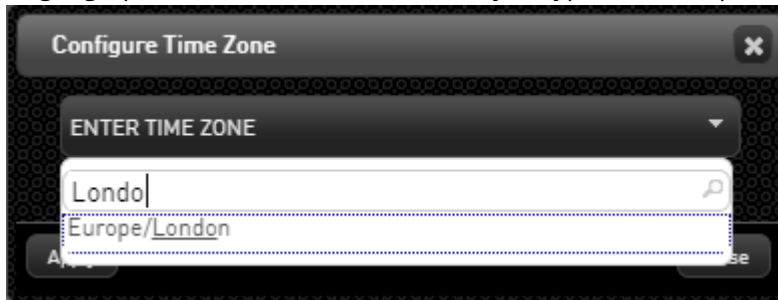
In the **Server Information** pane, click .

The **Configure Time Zone** popup opens.



1.

Open the dropdown list and select the required time zone. Alternatively, enter the name of a city or geographic area. The list is filtered as you type, for example:

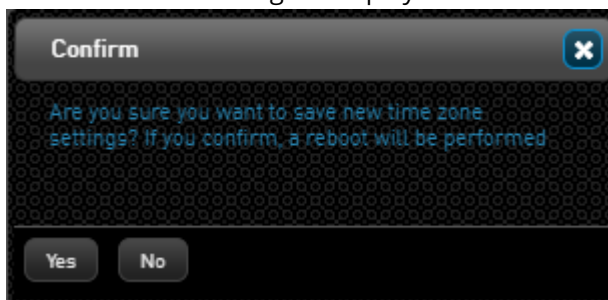


2.

Confirm your selection by clicking it (or by pressing **<Enter>**).

Click **Apply**.

A confirmation message is displayed.



3.

4. Click **Yes**.

Following an automatic reboot, the server time zone is reset.

Working with the Detection and Response Monitoring Environment Dashboard

Detection and Response Monitoring Environment Dashboard Overview

The Detection and Response Monitoring Environment Dashboard provides a snapshot of all detected malicious activities and infected endpoints reported to a Detection and Response Server during a specific period of time. The Dashboard view allows you to view, monitor and investigate all security alerts, and handle them according to your organization's requirements.

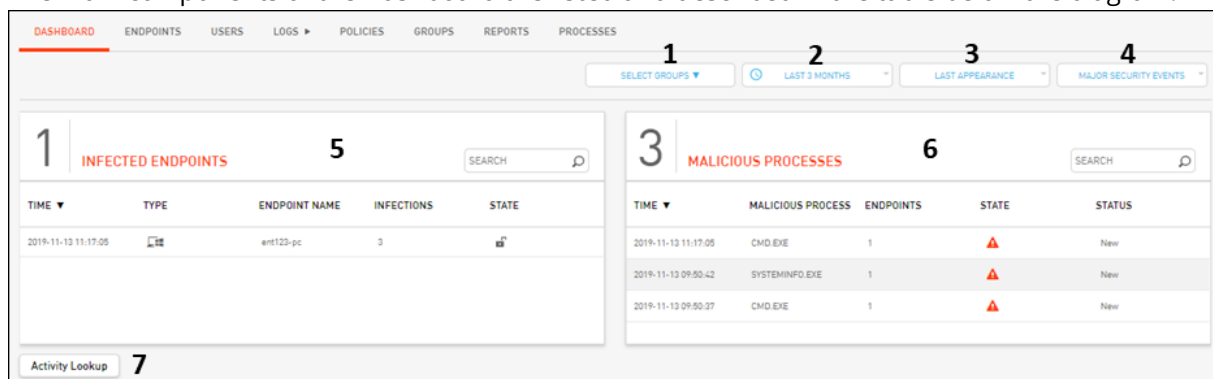
Some functionalities offered by the Dashboard include:

- Filtering of the lists according to search terms. Depending on the current view, you can filter according to endpoint name, malicious process name, Protection Module name, or deviant activity. You can also filter the view to show only the events that affected selected endpoints Groups.
- Easy access to reliable [information about the suspected malicious processes](#) that occurred during a specified timeframe (default is the past 24 hours).
- Detailed [drill down views](#) that provide data about each identified malicious process. This information includes a concise explanation of the deviant activity involved, a description of the potential security threat, and an indicator showing whether the process is the originator of the malicious activity.
- The ability to [manage detected activities](#) according to your security policies. For example, you might decide to allow certain activities that by default are blocked by the Detection and Response Agent. (For more information about configuring these types of rules, refer to [Policies Overview](#).)

Dashboard Interface

Following a successful login, the Dashboard view is displayed by default. If another view is currently displayed, access the Dashboard by clicking the **Dashboard** tab.

The main components of the Dashboard are listed and described in the table below the diagram.

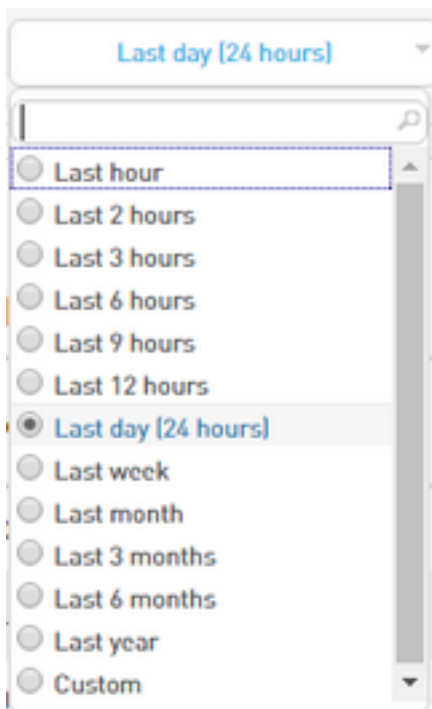


Number	Feature	Description
1	Groups filter	Enables you to filter the display to show only the events that affected one or more selected endpoints Groups.
2	Timeframe filter	Enables you to select the period of time for which to display data. By default, events from the past 24 hours are displayed.
3	Appearance sorter	Determines whether the dates/times displayed in the Dashboard are those when the malicious processes were first detected, or when they were noted most recently. <div data-bbox="529 573 932 786" data-label="Image"> <p>The image shows a dropdown menu for the 'Appearance' sorter. The menu is open, displaying two options: 'Last Appearance' (selected with a radio button) and 'First Appearance' (unselected with a radio button). The text 'Last Appearance' is highlighted in blue in the original image.</p> </div>
4	Events filter	Allows you to select one of the following views: <ul style="list-style-type: none"> • Major Security Events: This summary default view displays important events. • All Security Events: This view is recommended when performing analysis of events and activities.
5	Infected Endpoints frame	Displays a list of infected endpoints and the number of malicious processes detected on each one. For more information, refer to Infected Endpoints Summary .
6	Malicious Processes frame	Displays a list of malicious processes detected and the number of endpoints affected by each one. For more information, refer to Malicious Processes Summary .
7	Activity Lookup button	Enables you to search for information about a detected activity according to its identification number.

Selecting a Dashboard Timeframe

By default, the Dashboard displays events that have occurred in the past 24 hours. You can change this default setting to a shorter or longer time period, as required, using the Dashboard's time filter.

The time filter allows you to select a timeframe from a list of predefined options, or to define a customized timeframe. To select a predefined time period, open the time filter list and select the desired option.



The Dashboard summary is automatically refreshed according to the selected timeframe.

To define a custom time period:

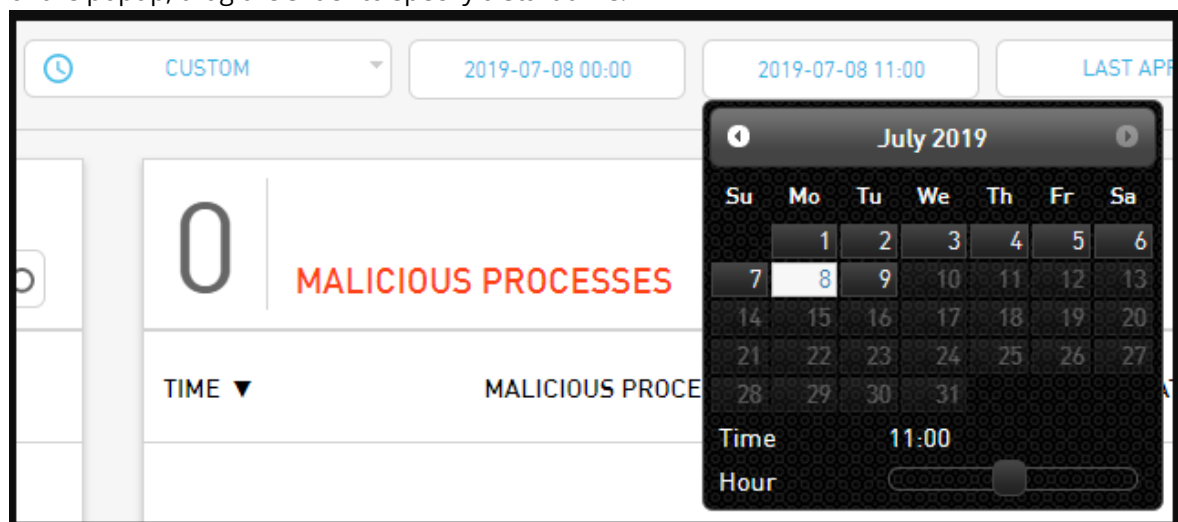
At the top of the Dashboard summary view, open the time filter list and select the **Custom** radio button.

Buttons for selecting the start and end times appear to the right of the Dashboard time filter.



- 1.
2. Click the button on the left to open a date picker popup.

From the date picker popup, navigate to and select the required start date. Then, at the bottom of the popup, drag the slider to specify a start time.



3. The date picker closes, and the selected date and time are displayed as the button label.










- Click the button on the right, and select a finish date and time.
The Dashboard summary is refreshed according to the custom timeframe.

Understanding the Detection and Response Monitoring Environment Dashboard Summary View

A malicious process is a process detected by Detection and Response that triggers one or more malicious activities on an Asset. The default Dashboard view shows a general summary of malicious processes that were detected during the specified timeframe, and the endpoints on which these processes were found.

Infected Endpoints Summary

This view shows the total number of Assets affected by malicious processes (4 in the example below), and lists the name (or IP address) of each Asset involved. By default, the list is sorted according to time of detection, with the most recent detection listed first. However, the list may be sorted (in either ascending or descending order) according to any column by clicking on the relevant column header.

4	INFECTED ENDPOINTS				SEARCH 
TIME ▼	TYPE	ENDPOINT NAME	INFECTIONS	STATE	
2019-05-05 01:20:45		DOTAN-LT	1		
2019-02-27 04:34:32		DESKTOP-UK1PN43	3		
2019-02-27 04:06:42		DESKTOP-100	4		
2019-01-24 01:10:16		ENT1-PC	1		

The **Infections** column indicates the total number of different malicious processes that occurred on the endpoint. The **State** column indicates the current mode of the Agent on the endpoint ([Detection](#) or [Prevention](#)).

The Search tool allows you to filter the **Infected Endpoints** list according to a key phrase contained in the name of one or more endpoints. The list is automatically filtered as you type the search term.

Selecting an endpoint (clicking on a row in the list) opens another view that lists all the malicious processes detected on that endpoint. This view enables you to [drill down to more detailed data](#) about the processes, such as the Protection Modules involved and the specific activities that constituted the security threat.

In the example below, three malicious processes were detected on the endpoint. The number on the far left of each row indicates the number of instances that were detected. The icon to the left of the process name indicates the [prevention state](#) of the malicious process. The icon to the right of the name indicates the security status of the malicious process, based on information from VirusTotal. For more details, refer to [Viewing Malware Information](#).

DASHBOARD DESKTOP-UK1PN43 X

ENDPOINTS: DESKTOP-UK1PN43





IP : 192.168.245.22 | STATUS: Prevention | GROUP NAME: Prevention, Workstations

3 MALICIOUS PROCESSES

[1]		CryLocker.exe	
[4]		69e966e730557fde8fd84317cde...	
[1]		powershell.exe	

Malicious Processes Summary

This view shows the total number of malicious processes reported during the selected timeframe (3 in the example below), and lists the name of each process involved. By default, the list is sorted according to time of detection, with the most recent detection listed first. However, the list may be sorted (in either ascending or descending order) according to any column by clicking on the relevant column header.

3	MALICIOUS PROCESSES				SEARCH 
TIME ▼	MALICIOUS PROCESS	ENDPOINTS	STATE	STATUS	
2019-11-13 11:17:05	CMD.EXE	1		New	
2019-11-13 09:50:42	SYSTEMINFO.EXE	1		New	
2019-11-13 09:50:37	CMD.EXE	1		New	

The **Endpoints** column indicates the total number of Assets affected by the malicious process. The **State** column shows the prevention state of the malicious process:



Prevented



Warning (could have been prevented, had the Agent been in Prevention mode)



Detected

The **Status** column shows the classification or current level of processing of the security incident:

- **New:** Event handling has not yet begun.
- **Confirmed Malware:** The process has been confirmed malicious by a Security Analyst.
- **Known Malware:** The process is recognized as malware in VirusTotal.
- **Under Investigation:** The incident has been referred to a Security Analyst for further study.
- **Awaiting Customer:** Has been reported and is waiting for customer response.
- **Blocked Software:** The process is prohibited for use in the organization, per request of the customer.

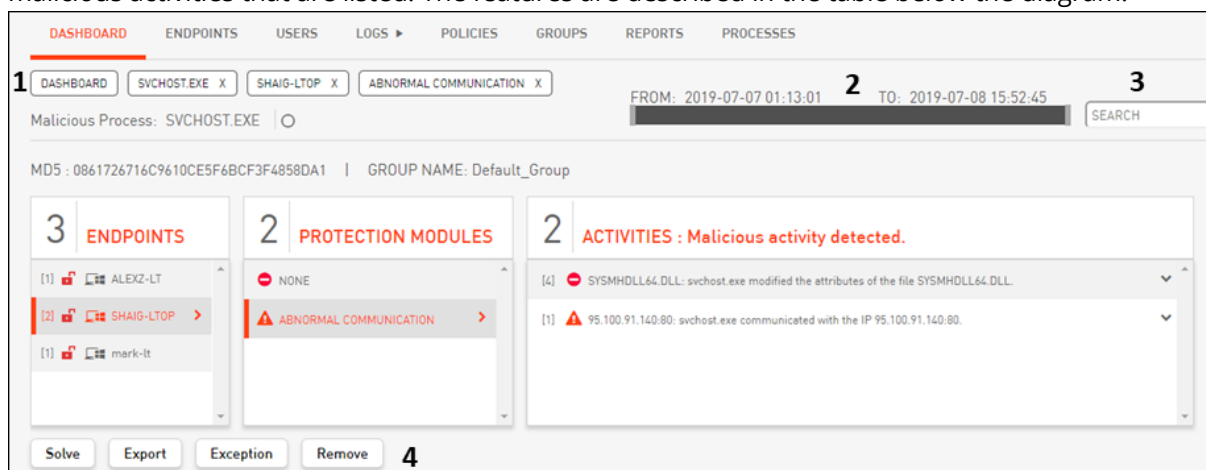
The Search tool allows you to filter the Malicious Processes list according to a key phrase contained in the name of one or more of the processes. The list is automatically filtered as you type the search term.

Selecting a malicious process (clicking on a row in the Malicious Processes list) opens another view that lists all the endpoints affected by that process. This view enables you to [drill down to more detailed data](#) about the relevant malicious process, such as the Protection Modules involved and the specific activities that constituted the security threat.

Drilling Down to Detailed Dashboard Data

The detailed Dashboard view (Drill Down view) provides additional data about a single malicious process. Drilling down displays the Protection Modules that detected the process and shows you all the deviant activities comprising the process.

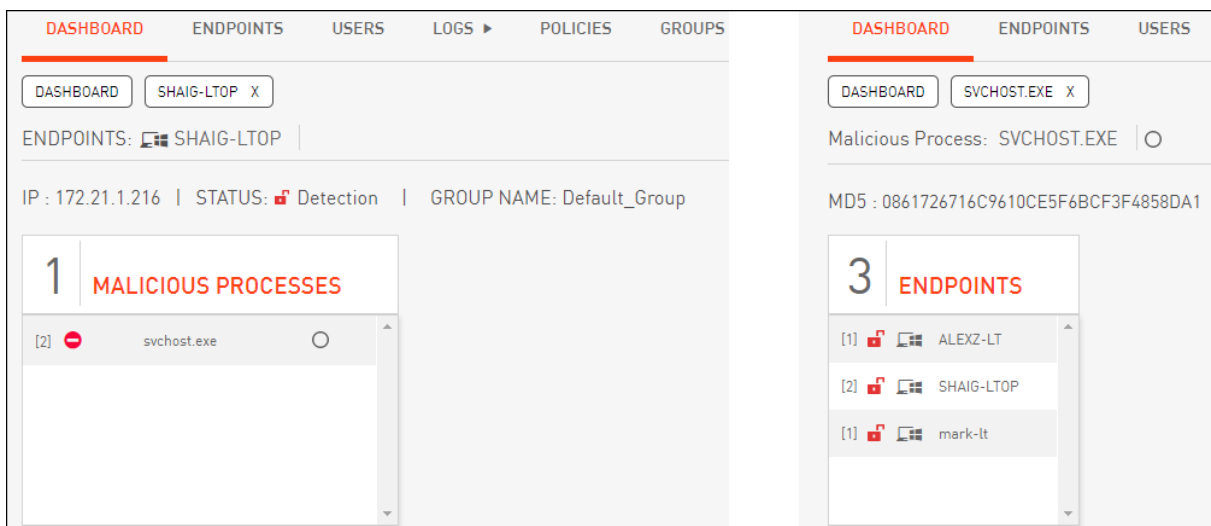
The Drill Down view includes several features to help you find relevant information and manage the malicious activities that are listed. The features are described in the table below the diagram.



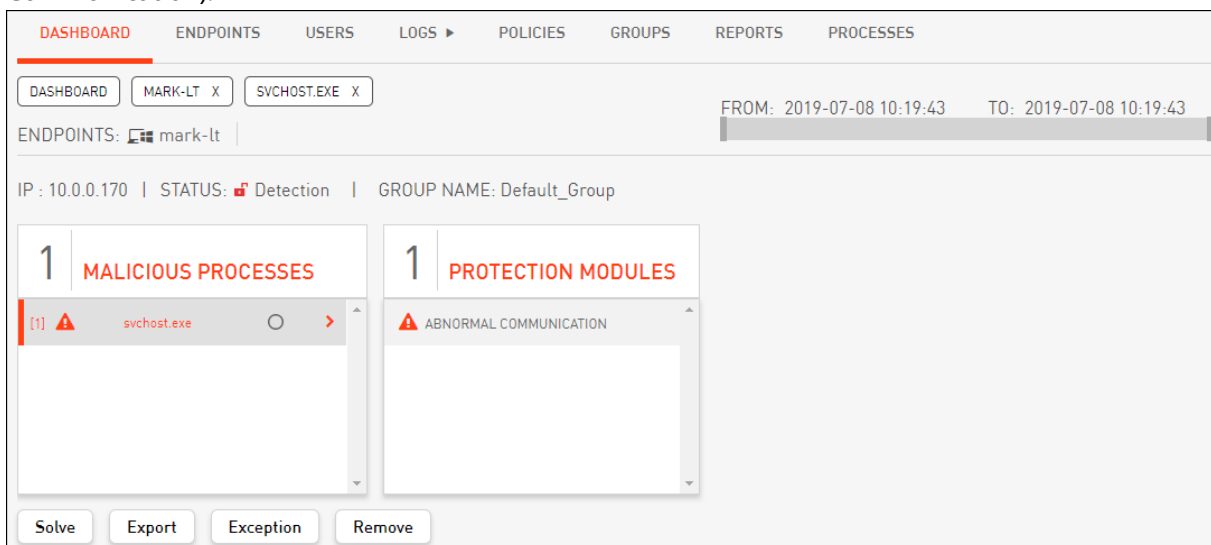
Number	Feature	Description
1	Breadcrumbs path	These buttons represent the current drill down path. Closing any of them (by clicking X) hides the relevant frame. Clicking the Dashboard button automatically re-opens the Dashboard summary view .
2	Timeframe bar	Displays the currently selected time period for which data is displayed.
3	Search tool	Enables you to filter the current view according to a search term. In full Drill Down view, you may filter by endpoint name, malicious process name, Protection Module name or activity name. The Dashboard is automatically filtered as you type the search term.
4	Administrative action buttons	These buttons allow you to manage the activities displayed in the Dashboard. For details, refer to Handling Events in the Dashboard View .

How to Drill Down

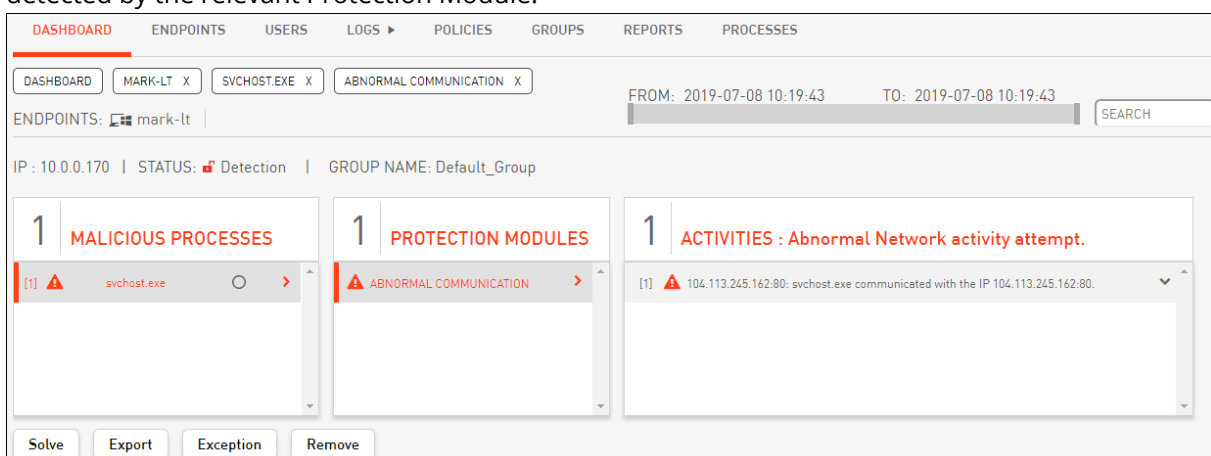
Access the Drill Down view by clicking on a malicious process or an endpoint name. You can start either from the **Malicious Processes** frame (when viewing infected endpoints) or from the **Endpoint Name** frame (when viewing malicious processes).



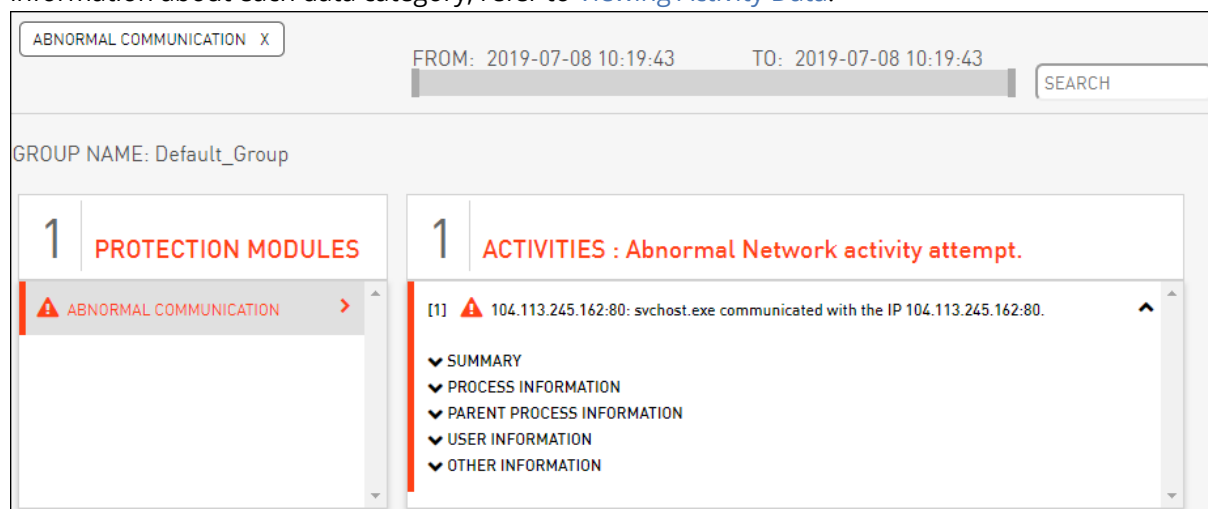
Selecting a malicious process or an endpoint name opens the **Protection Modules** frame. In the following example, the malicious process impacted one Protection Module (Abnormal Communication).



Selecting a Protection Module opens the **Activities** frame, which lists all the deviant activities detected by the relevant Protection Module.

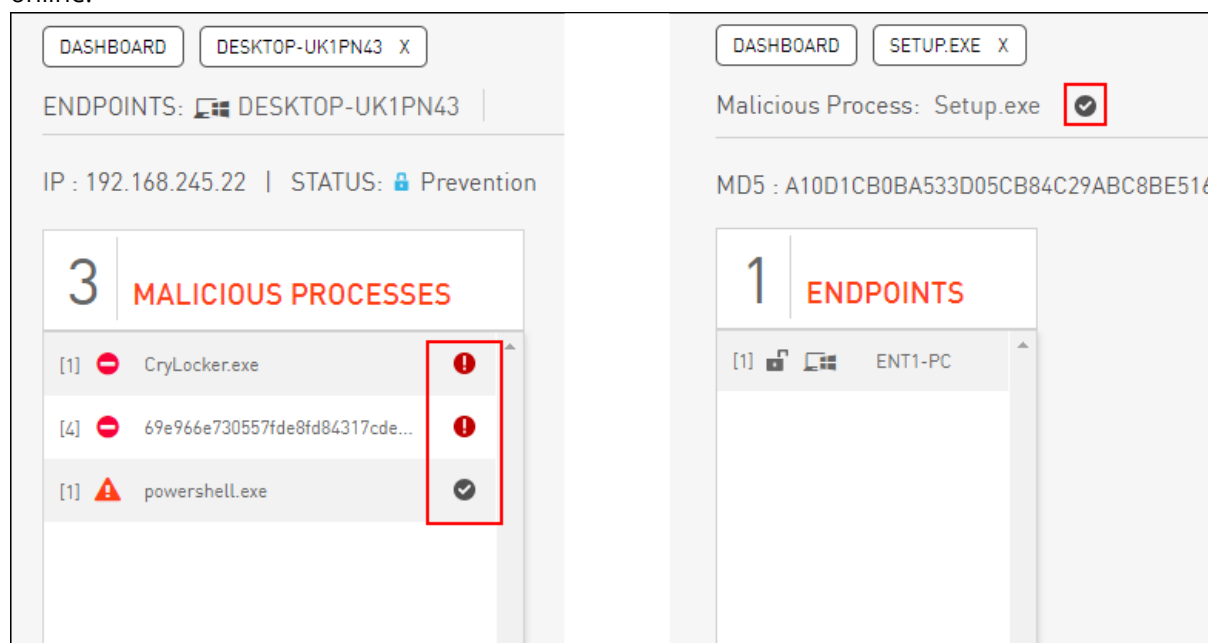


Finally, selecting an activity opens a pane that provides detailed data about the activity. For more information about each data category, refer to [Viewing Activity Data](#).







Viewing Malware Information

In the Detection and Response Monitoring Environment Dashboard's Drill Down view, malware information icons are displayed to the right of the name of each malicious process. The icons indicate the security status for the malicious process, based on malware information available online.

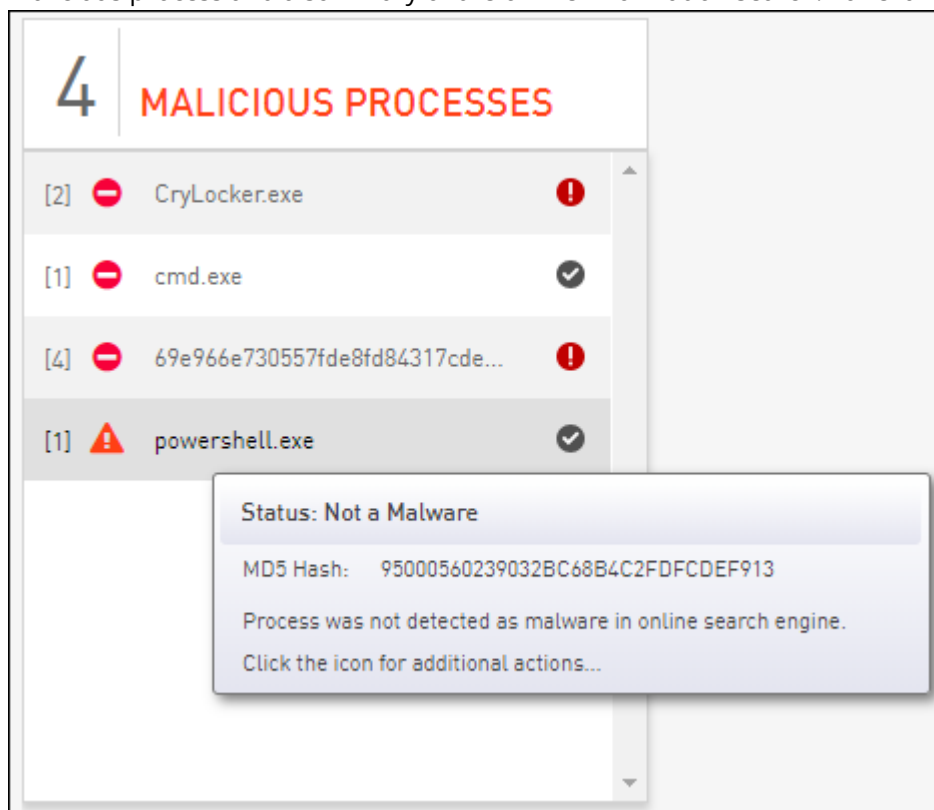


The security statuses are:

Icon	Status	Description
	Malware status not checked	An online search has not yet been performed.

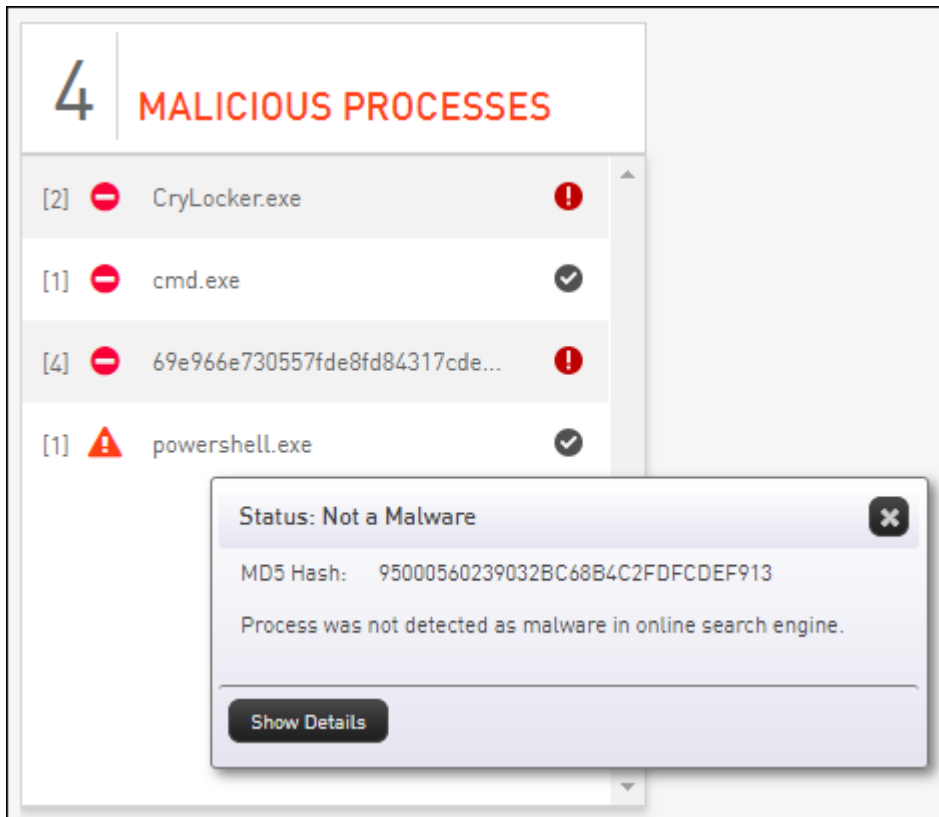
Icon	Status	Description
	No Internet connectivity	The server is unable to search for information due to lack of Internet access.
	No malware information	A search was done, and no online information was found about the process.
	Not a malware	A search was done, and the process was found not to be a security threat.
	Malware	A search was done, and at least one antivirus application classified the process as a security threat.

Hovering the mouse over the malware information icon displays the MD5 identifier for the malicious process and a summary of the online information search. For example:

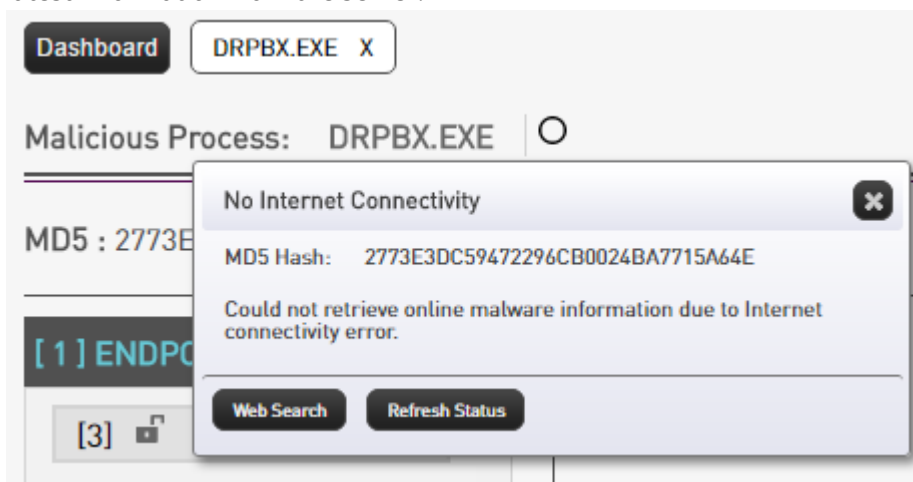


Clicking the malware information icon opens a popup that provides the following additional options:

- **Show Details:** Clicking this button opens a new browser tab displaying VirusTotal's findings about the process according to its MD5 identifier.



Refresh Status: Clicking this button updates the security status of the malicious process with the latest information from the server.




Viewing Activity Data

Selecting an activity from the **Activities** pane in the full Drill Down view of the Dashboard opens a frame that provides detailed data about the activity. Click each portion of the data to expand it and view its information.

1

ACTIVITIES : Abnormal Network activity attempt.

[1]  216.58.213.174:443: powershell.exe communicated with the IP 216.58.213.174:443.

✓ SUMMARY

✓ PROCESS INFORMATION

✓ PARENT PROCESS INFORMATION


✓ USER INFORMATION

✓ OTHER INFORMATION

Activity data includes:

SUMMARY: Provides a concise explanation of the deviant activity and the potential security threat. The Tainted Process indicator provides data about the root cause of the activity. A Tainted Process is a process that became compromised as a result of being manipulated by another process. A Tainted Process status of **No** indicates that this process is the originator of the malicious activity.

- The summary also lists additional basic information, such as the affected username, domain name, and timestamps for the event in both the Server's time zone and the endpoint's time zone. **No**

[1]  216.58.213.174:443: powershell.exe communicated with the IP 216.58.213.174:443.

^ SUMMARY

DESCRIPTION: The process C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe attempted to connect with the IP 216.58.213.174 via port 443. This communication may be a part of an attack, intended to provide the attacker with useful command and control information.

ADDRESS: 216.58.213.174:443

HOSTNAME: par21s04-in-f14.1e100.net

TIME: 2019-02-26 06:57:18

ENDPOINT'S LOCAL TIME: 2019-02-26 06:57:18

USER NAME: PC

USER DOMAIN NAME: SYSTEM

TAINTED PROCESS: YES

✓ PROCESS INFORMATION

✓ PARENT PROCESS INFORMATION

PROCESS INFORMATION: Provides a list of details about the malicious process, including the process MD5.

^ PROCESS INFORMATION

PATH: C:\WINDOWS\SYSWOW64\REG.EXE

TIME: 2019-11-13 09:47:44 - 2019-11-13 09:47:45

PROCESS MD5: AD7B9C14083B52BC532FBA5948342B98

PROCESS PATH: C:\Windows\SysWOW64\cmd.exe

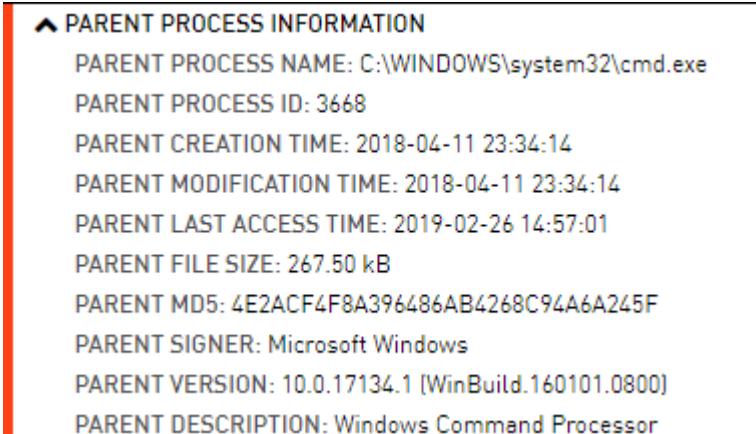
PROCESS ID: 2924

THREAD ID: 1484

CREATION: 2014-02-18 21:11:56

COMMAND LINE: C:\Windows\system32\cmd.exe /c C:\Users\qa\AppData\Local\Temp\...t24C5.tmp.bat

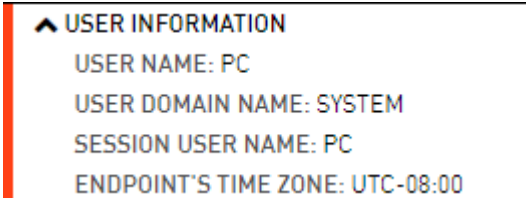
PARENT PROCESS INFORMATION: Provides a list of details about the parent process of the malicious process.

- 

^ PARENT PROCESS INFORMATION

 - PARENT PROCESS NAME: C:\WINDOWS\system32\cmd.exe
 - PARENT PROCESS ID: 3668
 - PARENT CREATION TIME: 2018-04-11 23:34:14
 - PARENT MODIFICATION TIME: 2018-04-11 23:34:14
 - PARENT LAST ACCESS TIME: 2019-02-26 14:57:01
 - PARENT FILE SIZE: 267.50 kB
 - PARENT MD5: 4E2ACF4F8A396486AB4268C94A6A245F
 - PARENT SIGNER: Microsoft Windows
 - PARENT VERSION: 10.0.17134.1 [WinBuild.160101.0800]
 - PARENT DESCRIPTION: Windows Command Processor

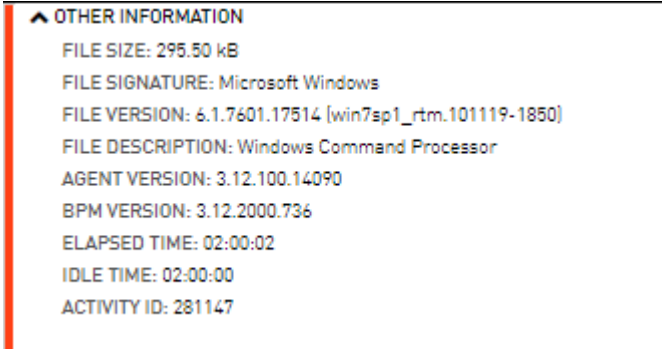
USER INFORMATION: Displays the user domain name, the username logged into the session, and the local time zone of the affected endpoint.

- 

^ USER INFORMATION

 - USER NAME: PC
 - USER DOMAIN NAME: SYSTEM
 - SESSION USER NAME: PC
 - ENDPOINT'S TIME ZONE: UTC-08:00

OTHER INFORMATION: Lists the Agent and BPM version, the Activity ID, and other additional relevant details related to the malicious process.

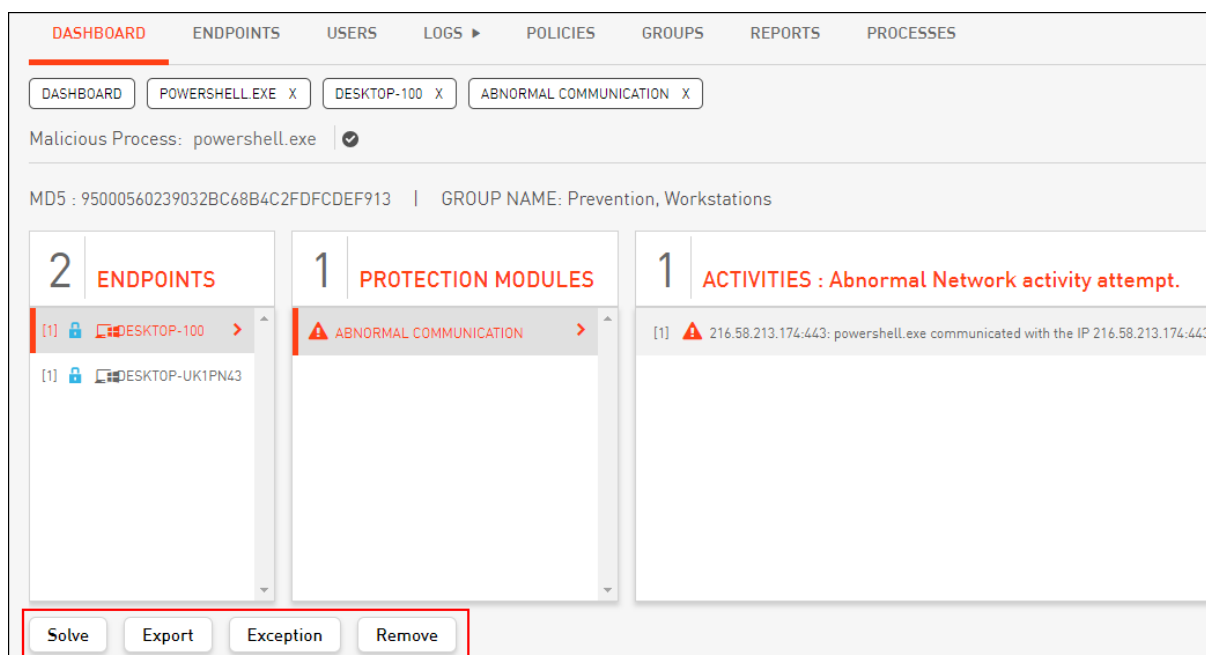
- 

^ OTHER INFORMATION

 - FILE SIZE: 295.50 kB
 - FILE SIGNATURE: Microsoft Windows
 - FILE VERSION: 6.1.7601.17514 [win7sp1_rtm.101119-1850]
 - FILE DESCRIPTION: Windows Command Processor
 - AGENT VERSION: 3.12.100.14090
 - BPM VERSION: 3.12.2000.736
 - ELAPSED TIME: 02:00:02
 - IDLE TIME: 02:00:00
 - ACTIVITY ID: 281147

Handling Events in the Dashboard View

The buttons in the lower left corner of the [Dashboard Drill Down view](#) enable you to perform actions related to managing events that are displayed in the Dashboard.



The options are:

Action	Description
Solve	Marks a selected event as having been resolved by an administrator. For details, refer to Resolving an Event .
Export	Saves selected Dashboard data as an XML file. For more information, refer to Exporting Dashboard Data .
Exception	Instructs Detection and Response to allow an event that by default would be blocked. For details, refer to Adding an Exception .
Remove	Deletes selected activity data from the Detection and Response database. For details, refer to Clearing Data from the Dashboard .

Events can be handled at the malicious process level, the Protection Module level, or the activity level. The impact of the administrative action is determined by the level of drill down that is currently selected:

- If only a malicious process is selected (there is no further drill down), the actions performed impact all components of the process, including all the Protection Modules and activities involved.
- If a Protection Module is selected, the actions performed affect all the activities connected to the selected Protection Module. However, there will be no impact on other Protection Modules and their activities.
- If a specific activity is selected, the actions performed impact only the selected activity.

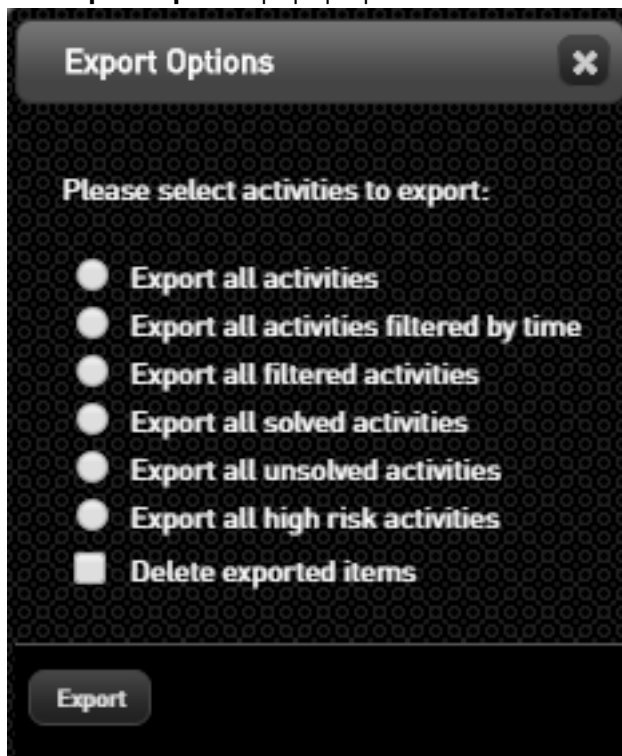
Exporting Dashboard Data

The Export action enables you to export some or all of the activities associated with a malicious process as an XML file. The file can then be imported to an external database and used for data comparison or analysis.

To export selected activities:

From the Dashboard, select the relevant event. Then, at the lower left corner of the page, click **Export**.

The **Export Options** popup opens.



- 1.
2. From the popup, select one of the radio buttons to specify which activities to export. (For information about solving activities, refer to Resolving Events, below.)
3. If you wish to remove the activities from the database following export, select the **Delete Exported Items** checkbox.
4. Click **Export**.

The popup closes, and the selected activities are exported to an XML file.

Clearing Data from the Dashboard

Selected data may be cleared from the Dashboard view in the following ways:

- **Resolving an event:** Records that the issue represented by the event has been handled and resolved.
- **Removing event activities:** Deletes the event from the database.

Resolving Events

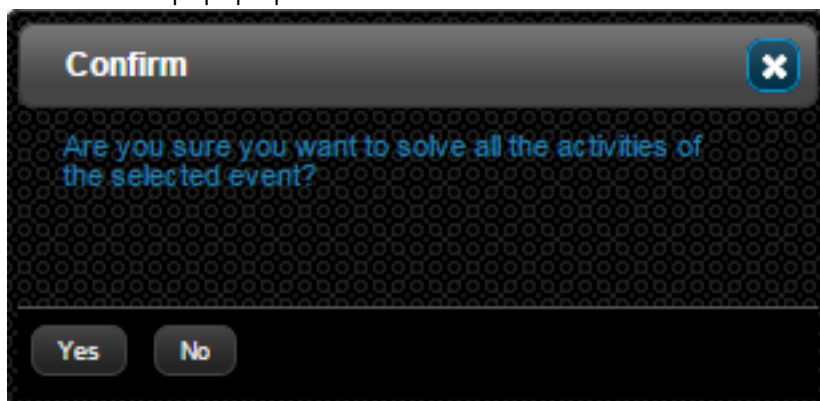
After you have investigated an event and taken the required actions to resolve the issue, you can use the Dashboard to mark the event as solved. Events can be solved at the activity level or at the malicious process level.

Solved events are automatically removed from the Dashboard view.

To solve an event:

From the Dashboard, select the relevant event. Then, at the lower left corner of the page, click **Solve**.

The **Confirm** popup opens.



- 1.
2. From the popup, click **Yes**.
The **Solution details** popup opens.
3. Enter a summary of how the event was addressed and handled. Then, click **Save**.
The popup closes, and the event is cleared from the Dashboard view.

Removing Event Activities

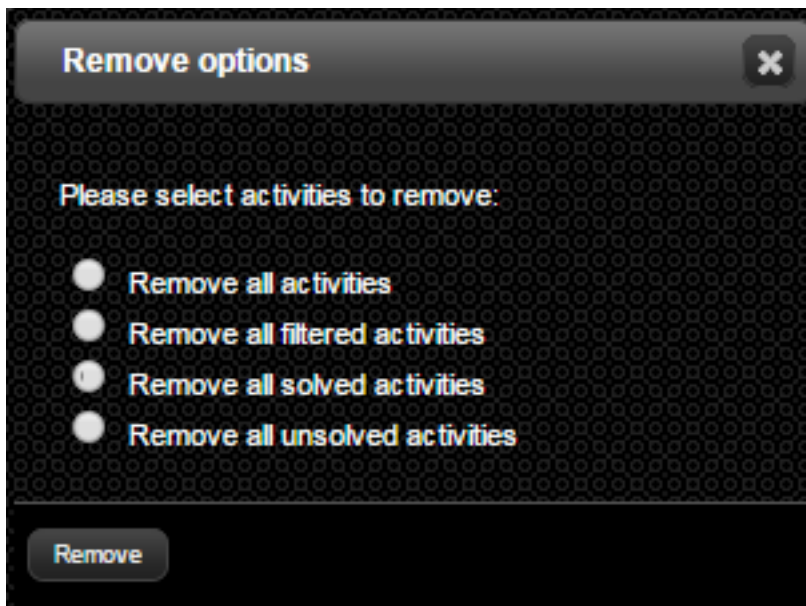
The Remove option enables you to delete selected activities from the Dashboard view. Removed data is also deleted from the Detection and Response database.

Warning!

It is generally not recommended to remove Dashboard events, particularly if you have not exported them.

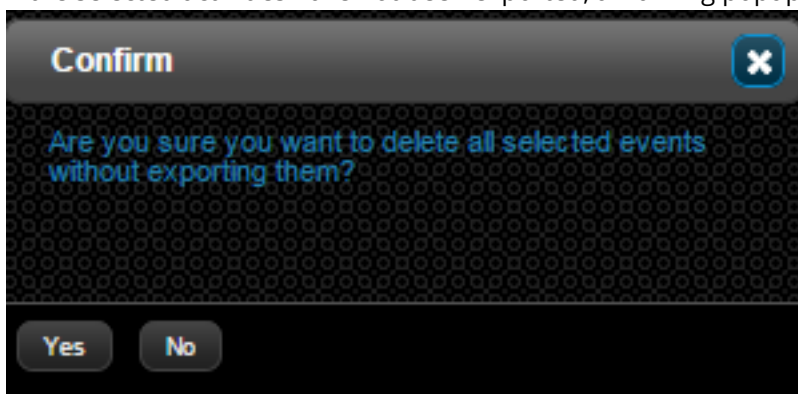
To delete Dashboard data:

1. From the Dashboard, select the relevant event. Then, at the lower right corner of the page, click **Remove**.
The **Remove options** popup opens.



2. From the popup, select one of the radio buttons to specify which activities to delete. Then, click **Remove**.

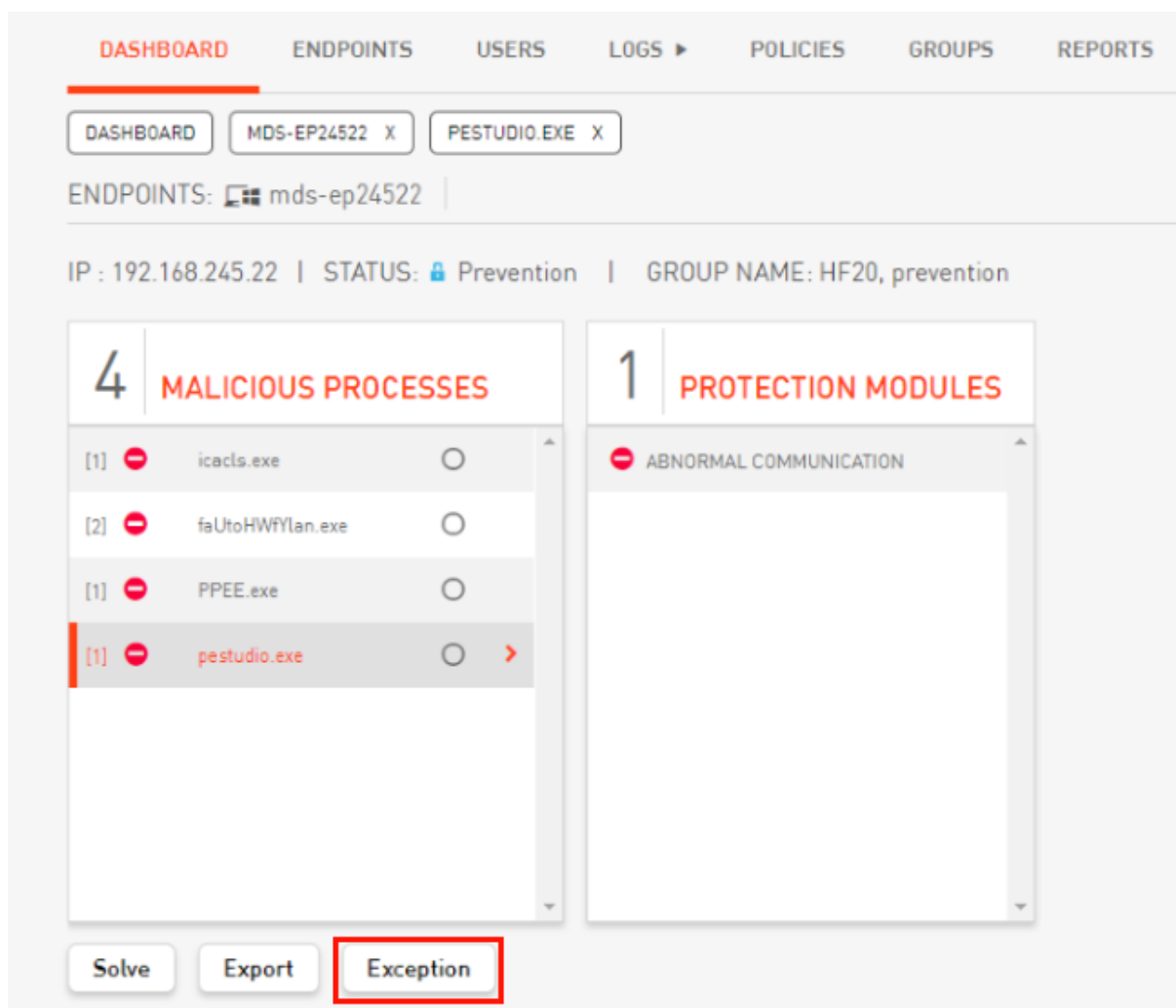
If the selected activities have not been exported, a warning popup opens:



- 3.
4. To continue, click **Yes**.
The popup closes, and the selected activities are deleted from the system.

Adding an Exception from the Detection and Response Monitoring Environment Dashboard

The **Exception** action is available in Drill Down view when a malicious process is selected. Use this option to create a rule permitting an action that would normally be blocked by Detection and Response.



Note

For more information about Exceptions and how to work with them, refer to [Viewing and Managing Exceptions in the Detection and Response Monitoring Environment](#).

When you click **Exception**, a dialog opens that allows you to create and assign the Exception. For convenience and to help prevent potential errors, some of the fields (e.g., Protection Module, Initiator Path, etc.) are pre-populated, based on the details of the selected event. You can modify any of these values as necessary.

Keep in mind that the number of prepopulated parameters varies according to the current level of drill down. At the Activity level, the greatest number of parameters will be prepopulated.

Edit Policy

▼ Policy Details

Name:

Description:

Protection Module:

Initiator Path:

Initiator Name:

Initiator Publisher:

Initiator MD5:

Initiator Command Line:

Parent Path:

Parent Name:

Parent Publisher:

Parent MD5:

Target Path:

Target Name:

► Assign Policy

Save Close

At the top of the dialog, enter a name for the Exception. Then, carefully review all the parameters. It is recommended to modify parameters such as paths to make them more generic, thus allowing the Exception to apply to other similar events. You can do this by using asterisks, which are wildcards that replace any other characters. For instance, in the example above you can make the Initiator Path ***\Users*\Desktop\Static\Basic\pestudio**

By default, new Exceptions are unassigned and do not affect event handling until they are assigned to endpoints. You can assign the Exception now or at any point after saving it, by opening the **Assign Policy** frame. For more information, refer to [Adding a Policy from the Policies Tab](#).

Using the Detection and Response Management Console Security Center

The Security Center: Overview

The state of the art Security Center of the Detection and Response Management Console lets you assess your organization's security status at a glance by providing a snapshot of malicious processes that are threatening your Assets. The intuitive, color-coded design enables you to quickly and easily identify the most dangerous processes and the Assets that are most at risk. The detailed drilldown views, which include Event Forensics, provide analysts with every detail necessary to understand and handle security incidents.

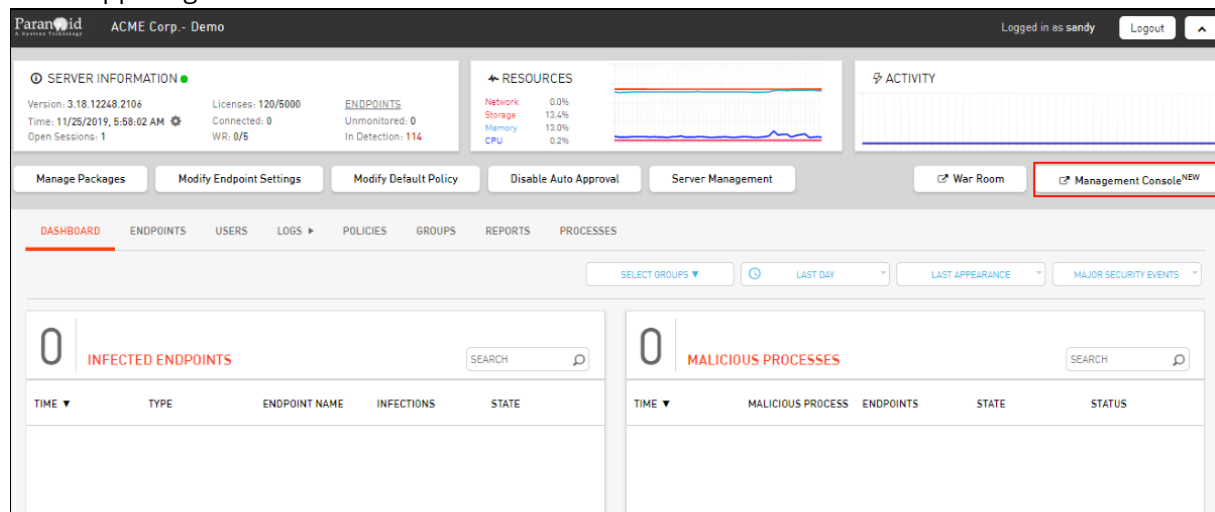
Data in the Security Center is automatically refreshed every 60 seconds.

The following sections describe the Security Center in more detail:

- [Accessing the Security Center](#)
- [Filtering the Display](#)
- [The Security Center Home Screen](#)
- [Security Center: Initial Drilldown](#)
- [Full Drilldown: Analyzing Incident Forensics](#)

Accessing the Security Center

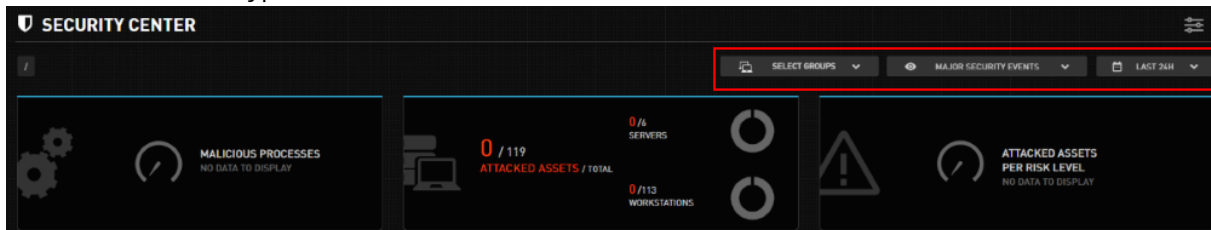
The Security Center is part of the new Detection and Response Management Console. To access it from the Detection and Response Monitoring Environment, click the **Management Console** button at the upper right side of the screen.



The Detection and Response Management Console, with the Security Center displayed by default, opens in a new browser tab,

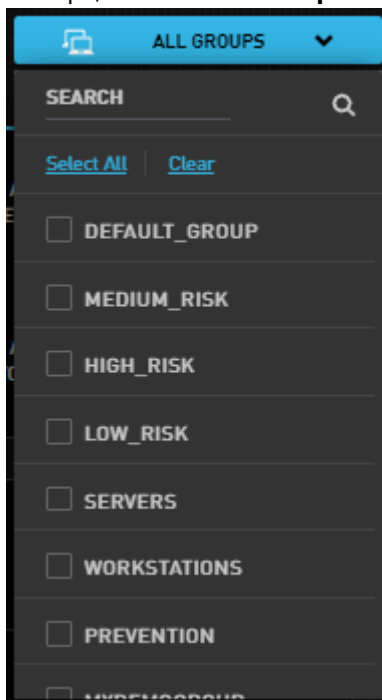
Filtering the Display

By default, the Security Center displays data related to major security events that occurred during the last 24 hours. The filtering options in the upper right corner of the Center enable you to adjust the timeframe, the types of events that are shown, and more.



The following filtering options are available:

Groups: By default, events affecting any Asset are displayed. To view events that affected certain Groups, click **Select Groups** and then choose the relevant Group(s) from the list.



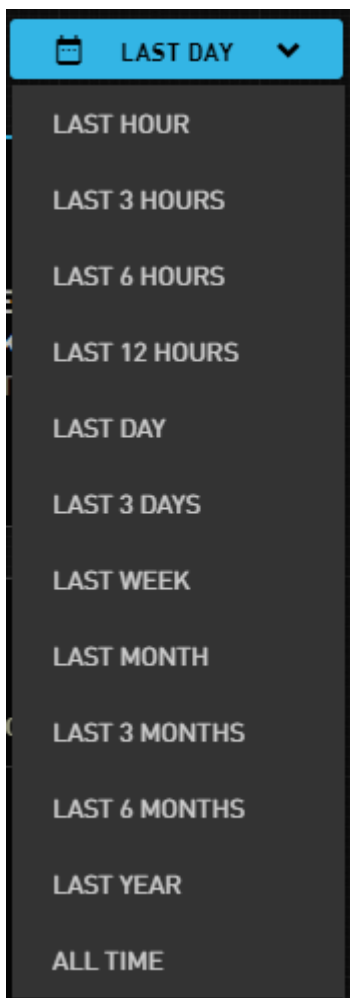
- **Event Type:** By default, Major Security Events are displayed. Alternatively, you can choose ONE of the following display options:
 - **All Security Events:** Provides a complete list of security incidents that occurred during the selected timeframe. This view, which is generally used during incident analysis, can contribute additional information that may help analysts to understand more about a security incident.
 - **Policy and Threat Alert Events:** This view lists events that violated [Hardening Policies](#) and

events that matched the queries defined in Threat Searches.

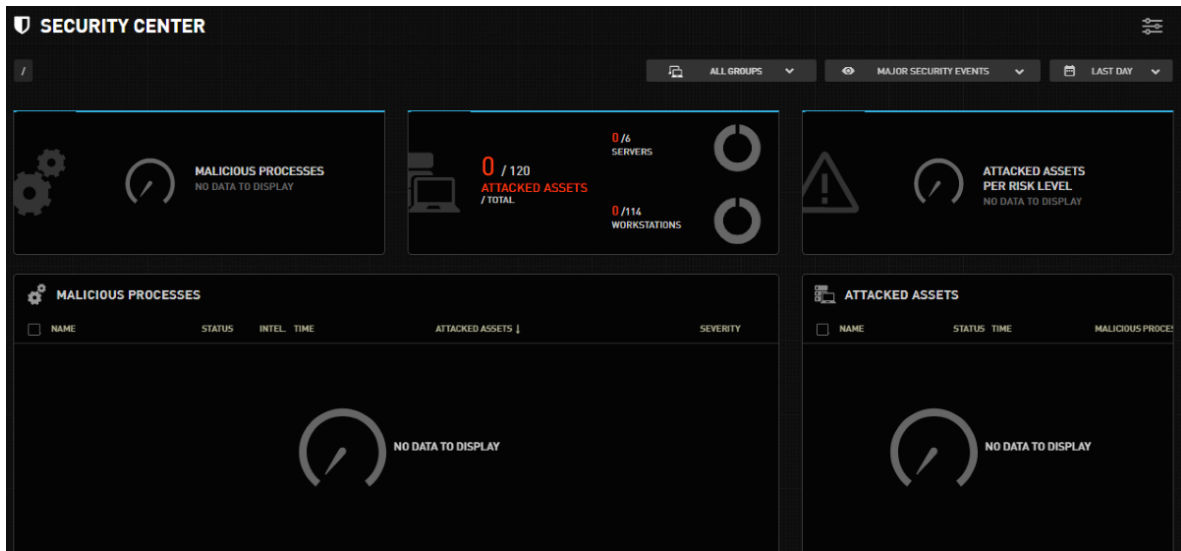
- **All Events:** Lists all security incidents as well as all policy and threat alert events.



Time: To change the time frame of data displayed, click the filter and select an option from the list.



If no data was collected during the selected timeframe, you will see the following screen:



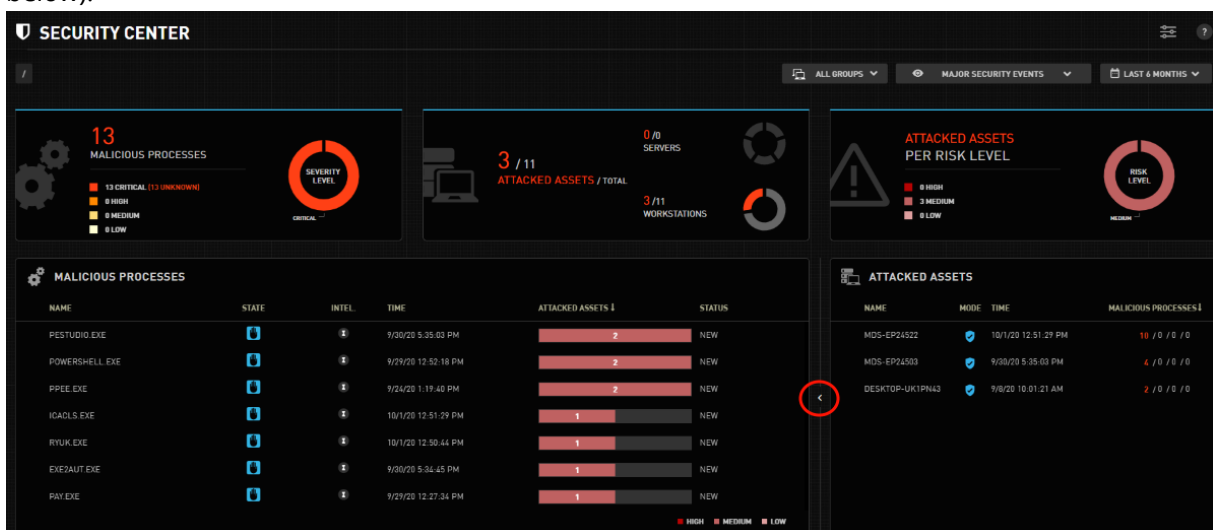
To view data, select an earlier timeframe.

Security Center Home Screen

The Home screen of the Detection and Response Management Console's Security Center presents a wealth of valuable data that allows you to quickly understand the overall security condition of your company's Assets. The information is organized to let you rapidly identify the processes that are most threatening to your organization and the Assets that are most at risk.

The Snapshot panels at the top of the Security Center provide a high-level breakdown of malicious processes and attacked Assets. The lower portion of the Security Center contains an [overview of Asset vulnerability](#). The most threatening malicious processes and the attacked Assets that are most at risk are displayed here.

For convenience, the **Malicious Processes** grid is wider than the **Attacked Assets** grid. To make the width of the two grids equal, click the arrow between the two grids (circled in red in the figure below).

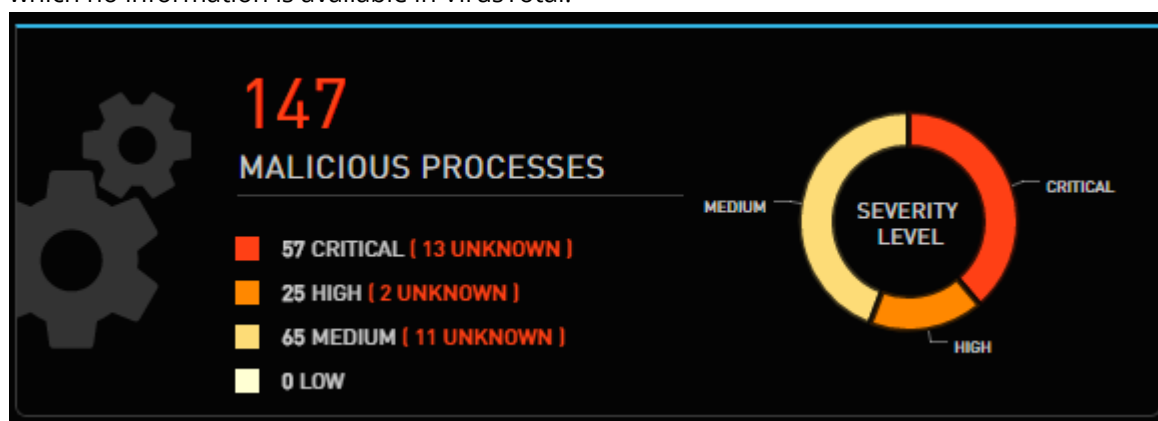


Security Snapshot Panel

The panel at the top of the Security Center shows the number of malicious processes reported and the number of Assets attacked during the selected timeframe. The total numbers displayed in the panel are adjusted according to the display filters selected and the current level of drilldown. For example, if you drill down according to a malicious process, only one malicious process (i.e., the one selected) will be shown.

The panel displays:

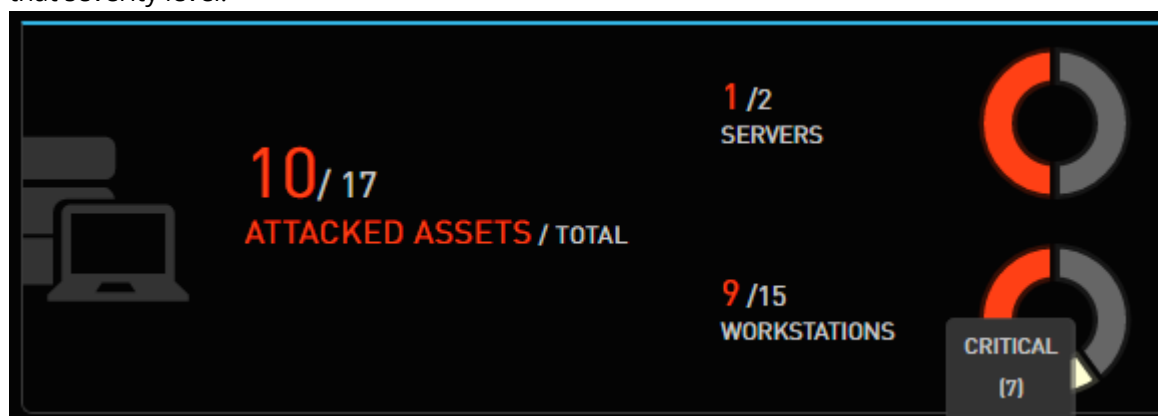
Malicious Processes: The total number of reported processes is broken down according to the severity of the events that they produced. Detection and Response calculates the severity level (Critical, High, Medium or Low) based on analysis of the activities that the process initiated. Unknown processes are those which are not classified as malware by VirusTotal, or for which no information is available in VirusTotal.



Note

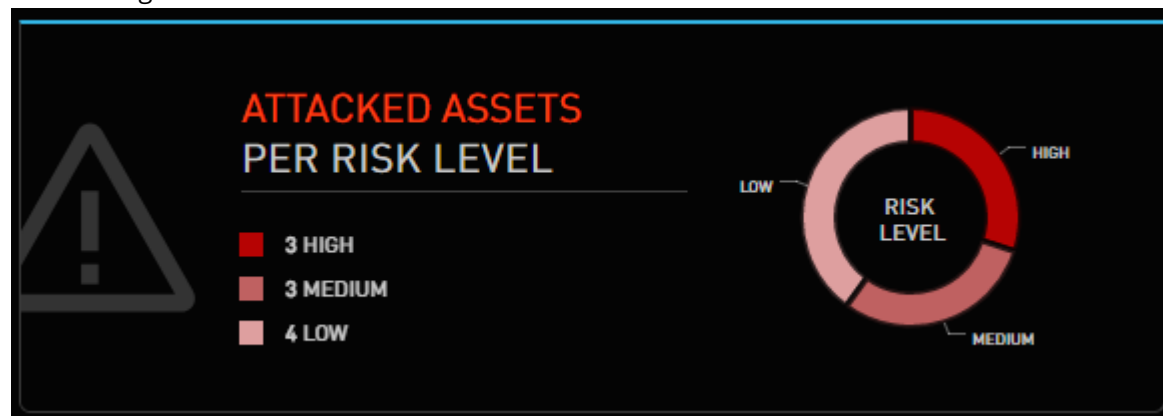
Processes can be categorized as Low only by Acronis Support or other professional analysts.

Attacked Assets/Total: Shows the number of Assets that sustained events relative to your total number of Assets. Assets are divided into servers and workstations, and the statistics are color-coded according to the severity of events that affected the Assets (Critical, High, Medium, Low). Hovering over a section of the donut chart displays the number of Assets affected by events of that severity level.



Attacked Assets per Risk Level: Shows total attacked Assets broken down according to the risk level of the Groups that the Assets belong to (High, Medium and Low). High risk level Groups generally contain Assets with more sensitive data (e.g., management).

Attacked Assets that belong to more than one Group are counted **once**, according to the Group with the highest level of risk.



Asset Vulnerability Overview






This part of the Security Center provides more detailed information about the processes that were reported and the Assets that were attacked. The data display is designed to help you focus on the most dangerous processes and identify the Assets that are most at risk.

The **Malicious Processes** view displays a list of the highest severity processes reported during the selected timeframe. The processes are sorted according to the Group risk level of affected Assets, and according to the number of events involved.

MALICIOUS PROCESSES						
NAME	STATE	INTEL.	TIME	ATTACKED ASSETS ↓	STATUS	
PESTUDIO.EXE			9/30/20 5:35:03 PM	<div><div>2</div></div>	NEW	
POWERSHELL.EXE			9/29/20 12:52:18 PM	<div><div>2</div></div>	NEW	
PPEE.EXE			9/24/20 1:19:40 PM	<div><div>2</div></div>	NEW	
ICACLS.EXE			10/1/20 12:51:29 PM	<div><div>1</div></div>	NEW	
RYUK.EXE			10/1/20 12:50:44 PM	<div><div>1</div></div>	NEW	
EXE2AUT.EXE			9/30/20 5:34:45 PM	<div><div>1</div></div>	NEW	
PAY.EXE			9/29/20 12:27:34 PM	<div><div>1</div></div>	NEW	

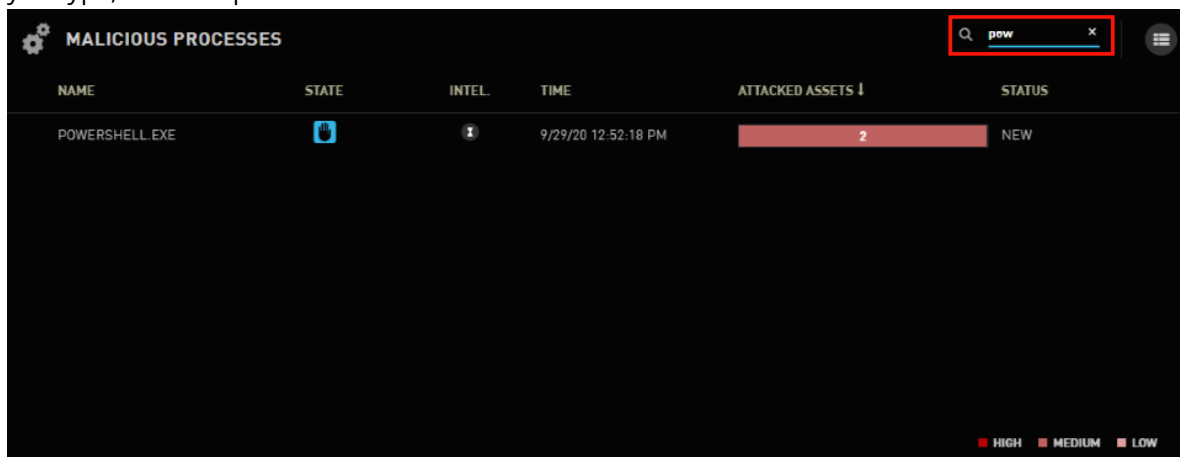
The following data is provided about each malicious process:

Column	Description
Name	Name of the malicious process.
State	These icons indicate how Detection and Response handled the process: <ul style="list-style-type: none"> Prevented: Malicious activities were prevented.

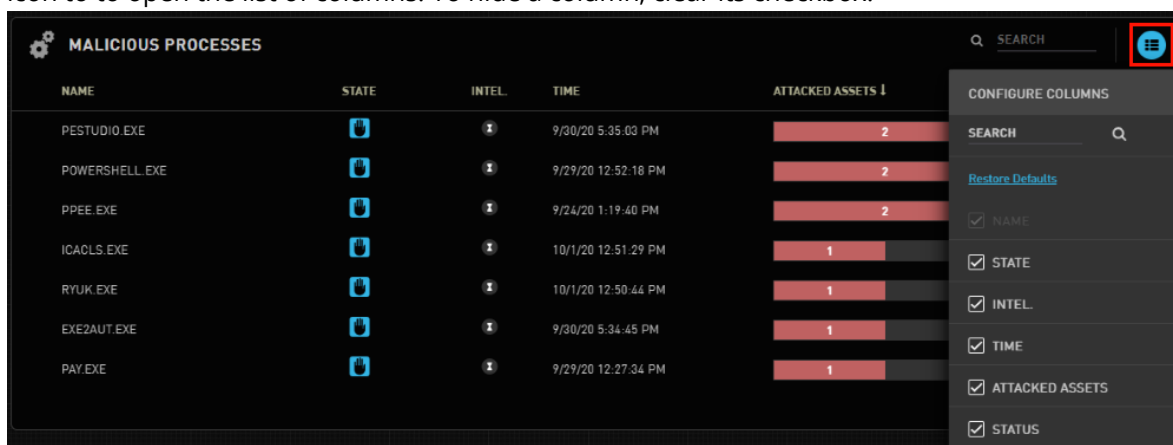
Column	Description
	<ul style="list-style-type: none">  Not Prevented: Malicious activities would have been prevented if the Asset had been in Prevention mode.  Detected: Some potentially malicious activities were detected.
Intel.	<p>These icons indicate process categorization according to VirusTotal:</p> <ul style="list-style-type: none">  Known as Malware: Classified as malware by VirusTotal.  Unknown to VirusTotal: No information available in VirusTotal.  Unknown as Malicious: Not classified as malware by VirusTotal, but is viewed by Detection and Response as a suspicious process.
Time	Timestamp of the most recent security incident.
Attacked Assets	The figures and colored bars show how many Assets were affected, broken down according to affected Assets belonging to Groups of High, Medium and Low risk levels.
Status	Current handling status of the security event (New, Reviewed, etc.).

When you hover over the **Malicious Processes** summary, the following features appear:

Search: Filters the Malicious Processes list according to an entered keyword. The list is filtered as you type, for example:



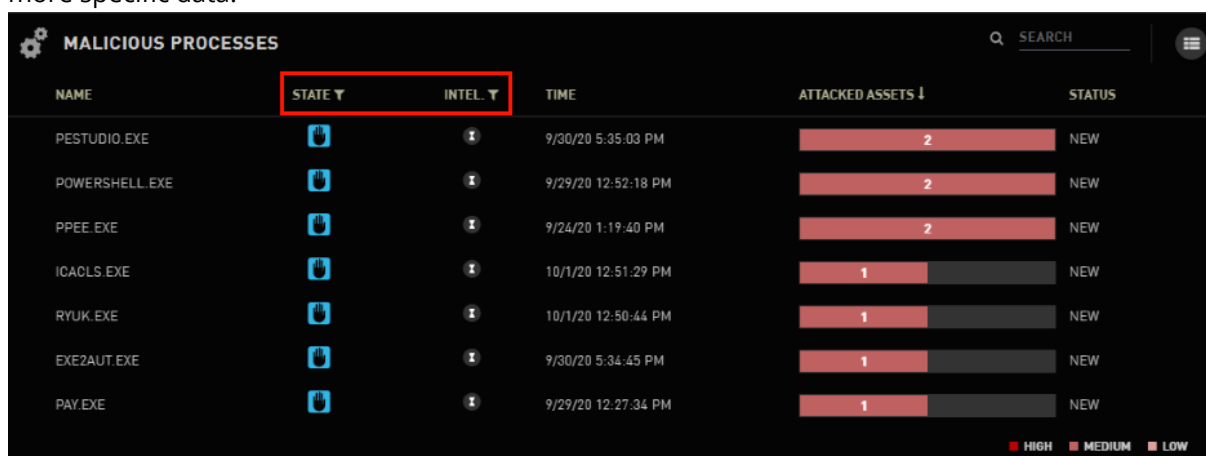
Configure Columns: This feature allows you to control the columns that are displayed. Click the icon to open the list of columns. To hide a column, clear its checkbox.



The screenshot shows the 'MALICIOUS PROCESSES' summary page. A red box highlights the 'Configure Columns' icon in the top right corner. The 'Configure Columns' menu is open, showing a list of columns with checkboxes: NAME, STATE, INTEL, TIME, ATTACKED ASSETS, and STATUS. All checkboxes are currently checked.

NAME	STATE	INTEL	TIME	ATTACKED ASSETS
PESTUDIO.EXE			9/30/20 5:35:03 PM	2
POWERSHELL.EXE			9/29/20 12:52:18 PM	2
PPEE.EXE			9/24/20 1:19:40 PM	2
ICACLS.EXE			10/1/20 12:51:29 PM	1
RYUK.EXE			10/1/20 12:50:44 PM	1
EXE2AUT.EXE			9/30/20 5:34:45 PM	1
PAY.EXE			9/29/20 12:27:34 PM	1

By default, the **Malicious Processes** summary lists processes of all states (**Prevented / Not Prevented / Detected**), and all intelligence classifications. (If a process involves multiple activities with different states, the highest state of intervention is displayed.) The Filter icons, which appear when hovering over the **State** and **Intel** columns, allow you to filter the summary so you can view more specific data.



The screenshot shows the 'MALICIOUS PROCESSES' summary page. Red boxes highlight the 'STATE' and 'INTEL' column headers, which have filter icons (downward arrows) next to them. The table below shows the data with a 'STATUS' column added.

NAME	STATE	INTEL	TIME	ATTACKED ASSETS	STATUS
PESTUDIO.EXE			9/30/20 5:35:03 PM	2	NEW
POWERSHELL.EXE			9/29/20 12:52:18 PM	2	NEW
PPEE.EXE			9/24/20 1:19:40 PM	2	NEW
ICACLS.EXE			10/1/20 12:51:29 PM	1	NEW
RYUK.EXE			10/1/20 12:50:44 PM	1	NEW
EXE2AUT.EXE			9/30/20 5:34:45 PM	1	NEW
PAY.EXE			9/29/20 12:27:34 PM	1	NEW

Legend: HIGH (red), MEDIUM (orange), LOW (green)

To filter the summary, click the Filter icons and then select the states and categories to be displayed. You can choose one or more filters.

MALICIOUS PROCESSES			
NAME	STATE	INTEL. ▼	TIME
PESTUDIO.EXE	<div> <div>SEARCH</div> <div> Select All Clear </div> <div> <input type="checkbox"/> KNOWN AS MALWARE </div> <div> <input type="checkbox"/> UNKNOWN TO VIRUSTOTAL </div> <div> <input type="checkbox"/> UNKNOWN AS MALICIOUS </div> </div>		9/30/20 5:35:03 PM
POWERSHELL.EXE			9/29/20 12:52:18 PM
PPEE.EXE			9/24/20 1:19:40 PM
ICACLS.EXE			10/1/20 12:51:29 PM
RYUK.EXE			10/1/20 12:50:44 PM
EXE2AUT.EXE			9/30/20 5:34:45 PM


The right side of the Asset Vulnerability Overview contains the **Attacked Assets** view, which lists affected Assets that are at highest risk. The Assets are sorted according to the severity level of the processes involved and the number of events that were generated.

ATTACKED ASSETS						
NAME	IP	MODE	DEPLOYMENT MODE	TIME	MALICIOUS PROCESSES ↓	RISK
MDS-EP24522	192.168.245.22		COMPLETED	10/1/20 12:51:29 PM	10	
MDS-EP24503	192.168.245.3		COMPLETED	9/30/20 5:35:03 PM	4	
DESKTOP-UK1P...	192.168.245.23		COMPLETED	9/8/20 10:01:21 AM	2	

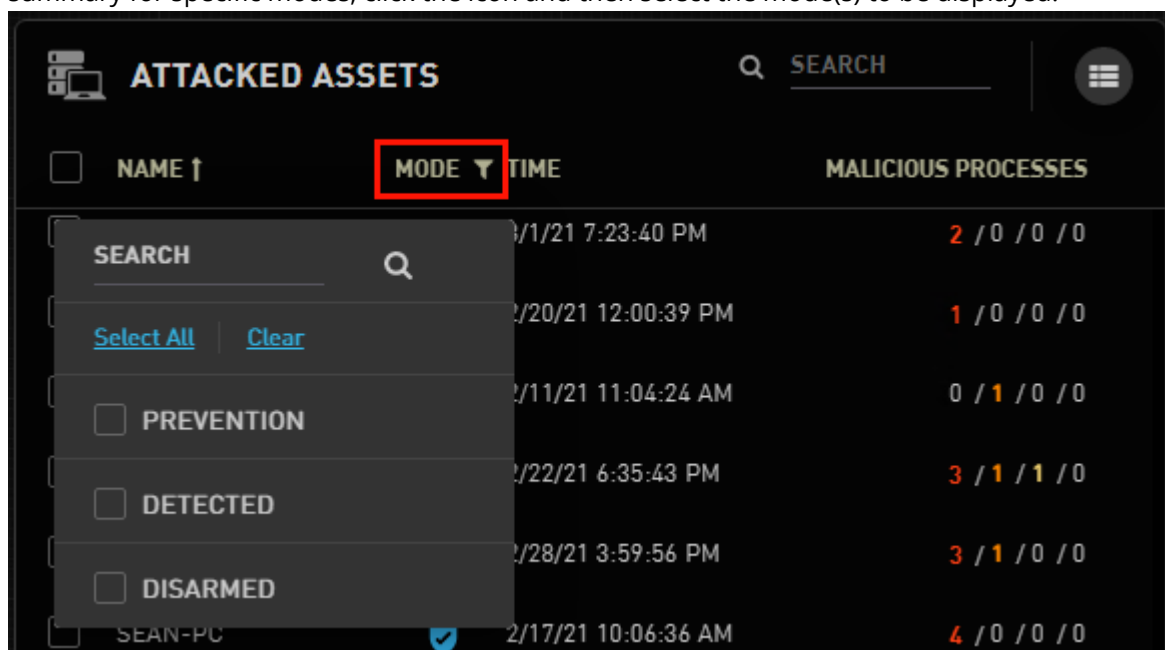
CRITICAL
 HIGH
 MEDIUM
 LOW

The following data is provided about each attacked Asset:

Number	Description
Name	Name of the Asset.
IP	IP address of the Asset.
Mode	<p>These icons indicate the current mode of the Agent on the Asset:</p> <ul style="list-style-type: none"> Asset is in Prevention mode. Asset is in Detection mode. Asset is currently Disarmed. When it is taken out of Disarmed mode, it will return to Prevention mode.

Number	Description
	<ul style="list-style-type: none">  Asset is currently Disarmed. When it is taken out of Disarmed mode, it will return to Detection mode.
Deployment Mode	Indicates whether Deployment Mode (a temporary stage relevant to newly deployed Assets) is still in progress or has been completed.
Time	Timestamp of the most recent security incident.
Malicious Processes	The figures and colored bars show how many malicious processes affected the Asset, broken down according to severity level of the processes (Critical, High, Medium and Low).
Risk	These color-coded icons indicate the risk level of the Group that the Asset belongs to (High, Medium or Low). If an Asset belongs to multiple Groups, the Group of the highest risk level takes priority.

The Search and Configure Columns features appear when you hover over the **Attacked Assets** summary. In addition, when you hover over the **Mode** column, a Filter icon appears. To filter the summary for specific modes, click the icon and then select the mode(s) to be displayed.



Note


Selecting a malicious process or an attacked Asset (by clicking the relevant row) opens a drill down view for the process or the Asset. For details, refer to [Security Center: Initial Drilldown](#).

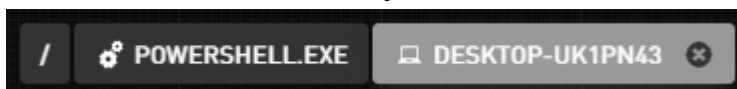
Detection and Response Management Console Security Center: Initial Drilldown

Selecting either a malicious process or an attacked Asset from the lists on the [Home screen](#) opens the initial drilldown view. In this view, all Security Center components display data related to the selected process or Asset only.

In any drilldown view (initial or full), the breadcrumbs path at the upper left corner of the Security Center reflects the selected process and Asset name, in the order that they were selected. For example:



To return to a previous level of drilldown, hover over the element that you want to close and click the Close icon. To return directly to the Home screen, click .



The sections below summarize the main aspects of an initial drilldown view:

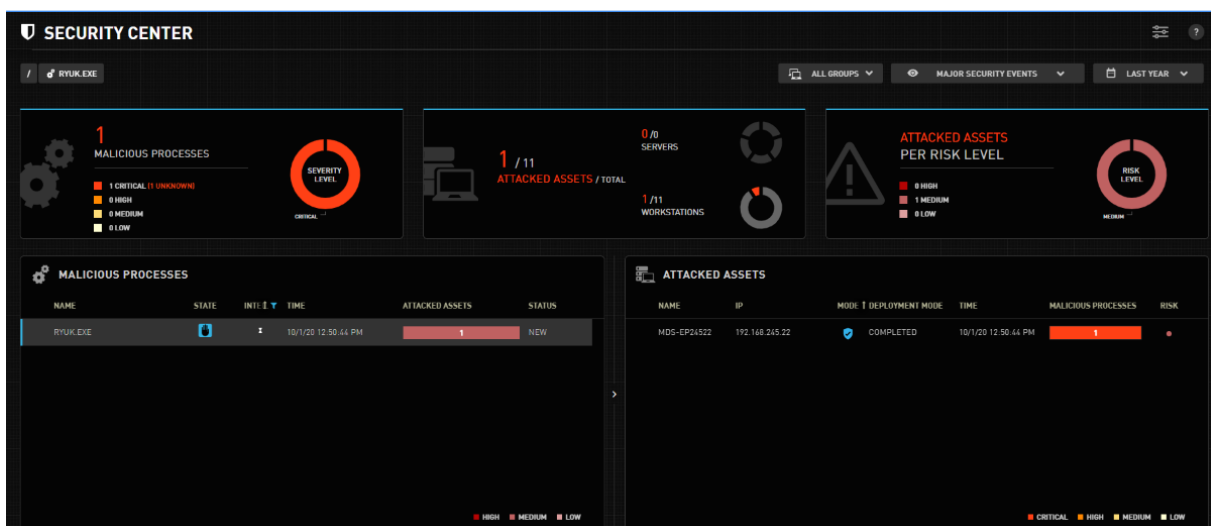
- [Malicious Process Drilldown](#)
- [Attacked Asset Drilldown](#)

Malicious Process Drilldown

When you select a malicious process, the process name appears in the breadcrumbs path at the upper left corner of the Security Center. Lists of attacked Assets are filtered for only those affected by the selected process, so you can quickly assess the impact of the process on your organization.

Note

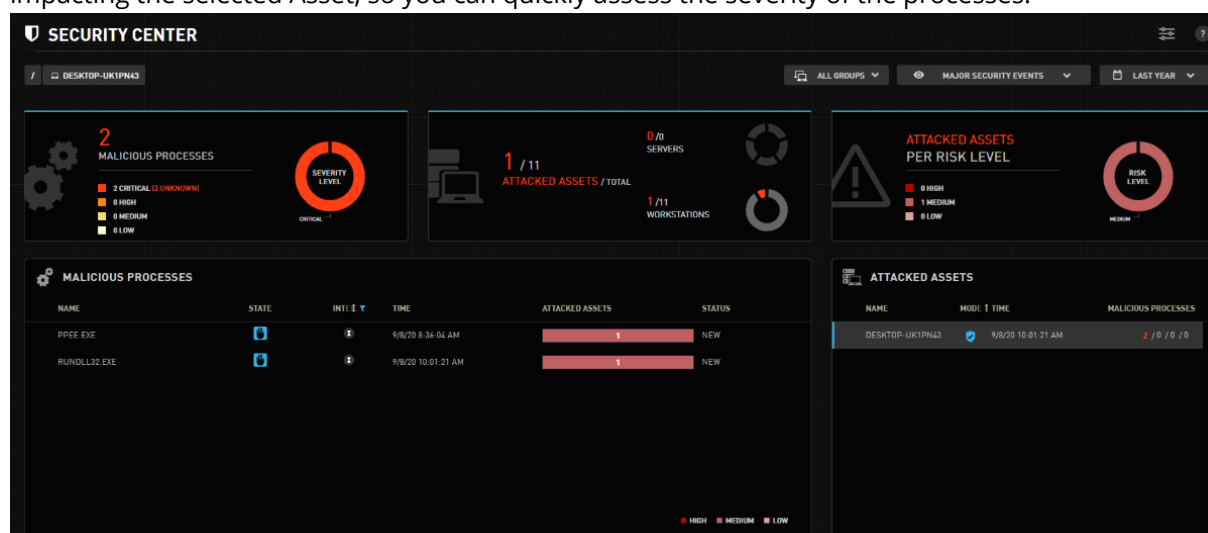
For detailed information about general components of the Security Center, refer to [The Home Screen](#).



Selecting a row in the Attacked Assets list opens a full drilldown view, where you can view details about each activity generated on the Asset by the process. For more information, refer to [Viewing Incident Forensics](#).

Attacked Asset Drilldown

When you select an attacked Asset, the name of the Asset appears in the breadcrumbs path at the upper left corner of the Security Center. Lists of malicious processes are filtered for only those impacting the selected Asset, so you can quickly assess the severity of the processes.



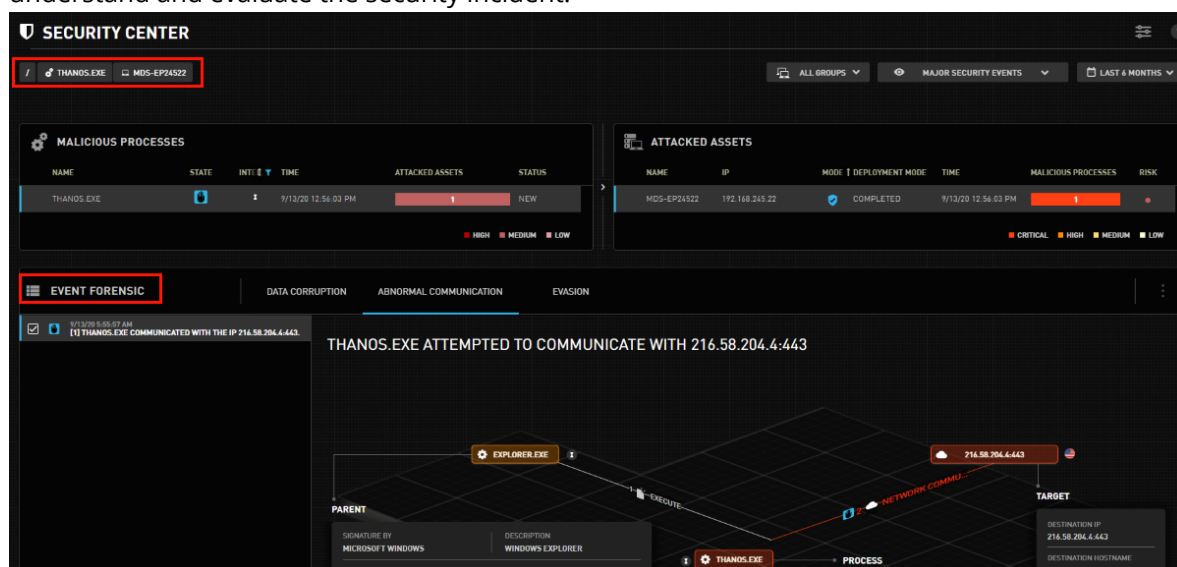
Selecting a row in the Malicious Processes list opens a full drilldown view, where you can view details about each activity generated by that process on the Asset. For more information, refer to [Viewing Incident Forensics](#).

Security Center Full Drilldown: Analyzing Incident Forensics

The full drilldown view is displayed when you select a process from the **Malicious Processes** list and an Asset from the **Attacked Assets** list. This view features the following elements:

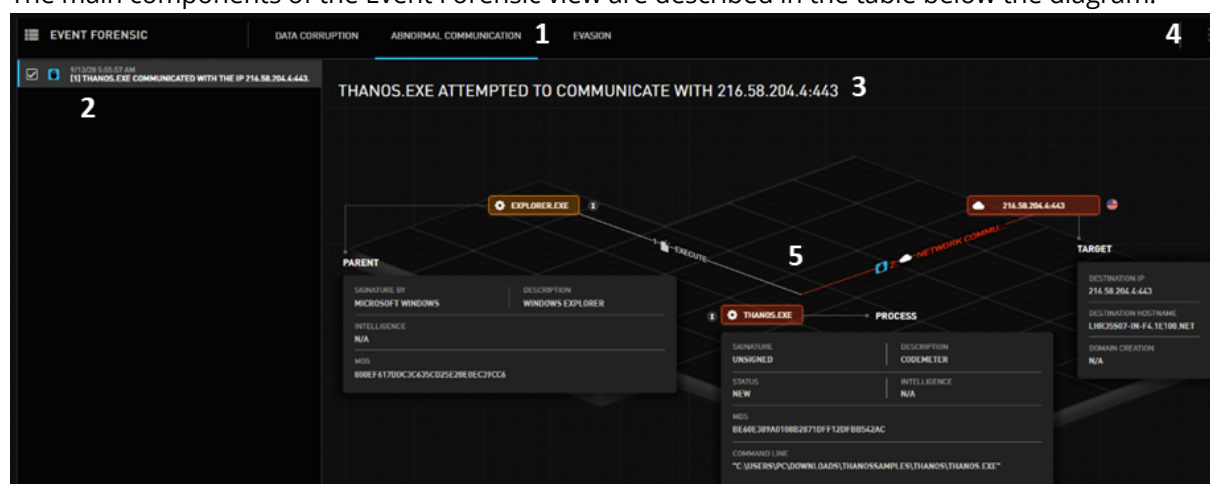
- The breadcrumbs path at the upper left corner of the Security Center includes the names of the selected process and Asset.
- All lists and charts are filtered for the selected process and Asset. For detailed information about these components, refer to [Security Center Home Screen](#).
- Event Forensic data is displayed below the Asset vulnerability summaries. The Event Forensic view lists all activities generated by the process and provides detailed information to help you

understand and evaluate the security incident.



The list of activities generated by the malicious process are categorized according to Protection Modules. Selecting an activity displays full details about that activity, including a Storyline graph that lets you easily visualize the flow of events involved.

The main components of the Event Forensic view are described in the table below the diagram.



Number	Component	Description
1	Protection Modules list	The Protection Modules associated with the generated activities are listed at the top of the Incident Forensics view. The currently selected Protection Module is indicated by a blue bar.
2	Activity list	A list of all activities generated during the selected timeframe. The currently selected activity is indicated by a blue bar.
3	Activity description	Provides a brief summary of the activity.
4	Display options icon	Click the icon to open a list of options. For details, refer to Incident Forensics: Display Options (below).


Number	Component	Description
5	Storyline	Depicts the flow of events involved in the activity. For more information, refer to The Event Forensic Storyline .


Incident Forensics: Display Options

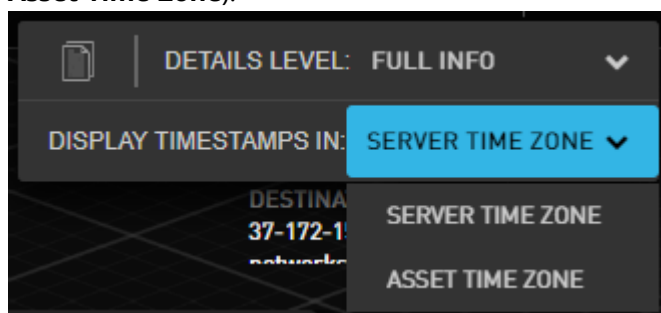
The following options are available for viewing Event Forensics:

- Time zone of timestamps
- Level of detail displayed

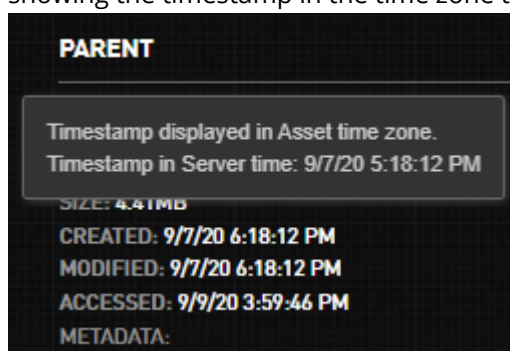
Selecting Displayed Time Zone

Event Forensics can be viewed in the time zone of either the Detection and Response server or the affected Asset. To check which time zone is currently being displayed, hover over the  icon in the upper right corner of the Event Forensic view. The currently selected time zone is shown in a tooltip.


To change the time zone display, click  and select the relevant option (**Server Time Zone** or **Asset Time Zone**).

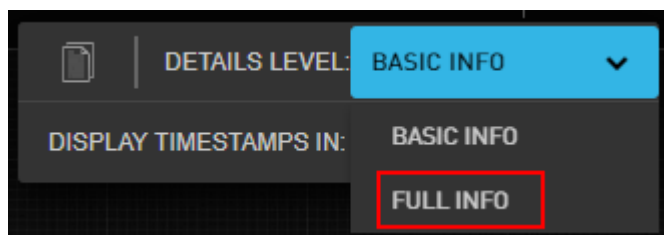


For convenience, hovering over any timestamp in the Incident Forensics Storyline opens a tooltip showing the timestamp in the time zone that is *not* currently selected. For example:

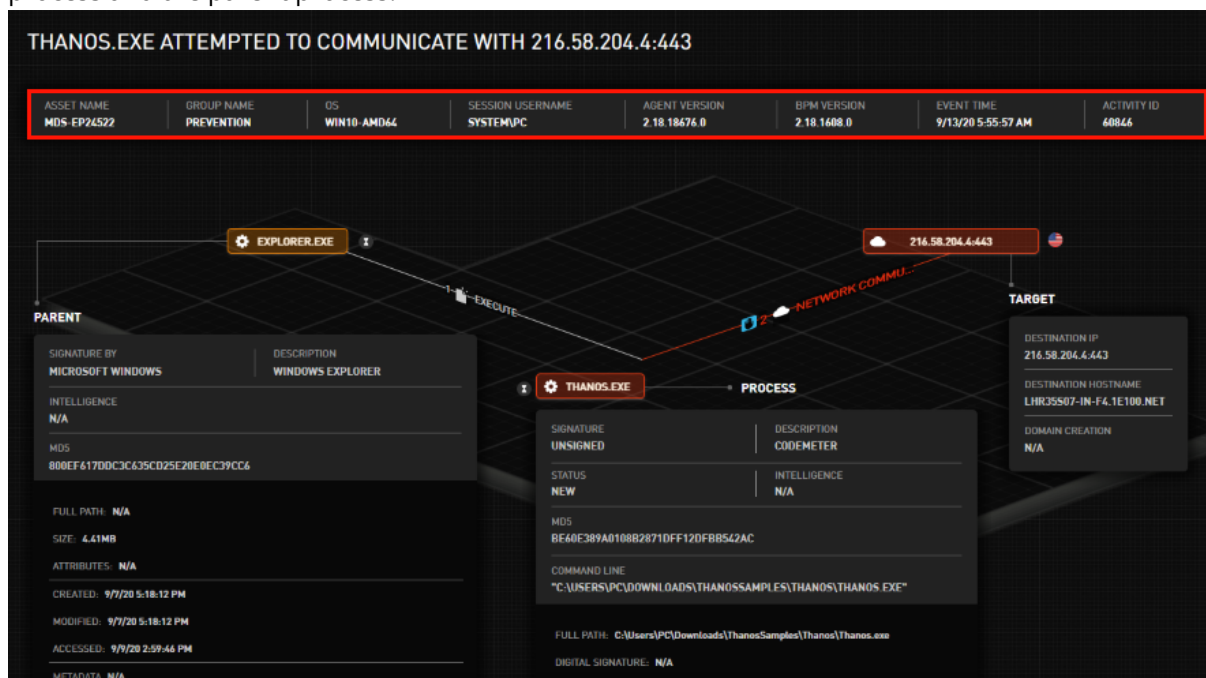


Selecting Level of Detail

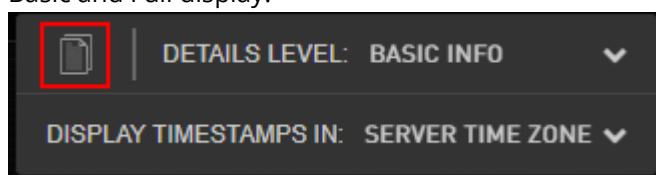
By default, the Event Forensic view displays basic details (as described below in [The Event Forensic Storyline](#)). To view additional details in the Storyline, click  and select **Full Info**.



The Full Info display features a header bar that shows relevant context information (such as Group name, OS, Agent / BPM version, Activity ID, etc.), and many more details are provided about the process and the parent process.



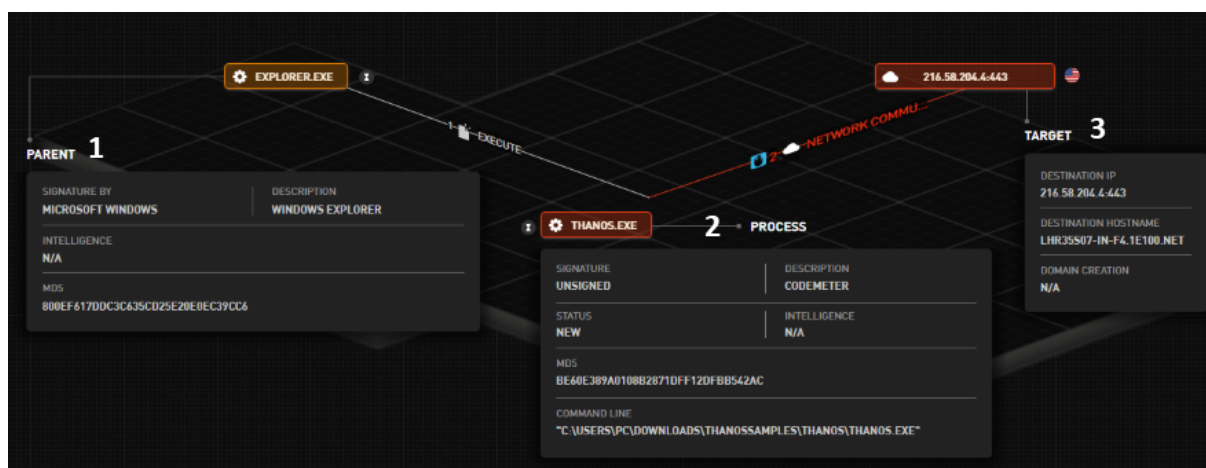
Clicking the Copy icon copies the Storyline details to your clipboard. The icon is available in both Basic and Full display.



The Event Forensic Storyline

The Storyline shows a linear graphic display of the sequence of events involved in the activity, including an indication of the point at which the activity was prevented or detected. In addition, detailed information is provided about the process, its origin and its target.

The different components of the Storyline are described in the table below the example.



Number	Component	Description
1	Parent	Details about the Parent process of the initiator process, including signature information, MD5 and data about online reputation.
2	Process	Details about the process that performed or attempted the malicious operation. The summary includes signature information, current event handling status, data gathered from cloud intelligence and more.
3	Target	Details about the intended target (e.g., file, registry key, IP address, etc.) of the malicious process. If the target is an IP address (as in the example above), the flag icon indicates the location of the IP.

Handling Endpoints in the Detection and Response Monitoring Environment

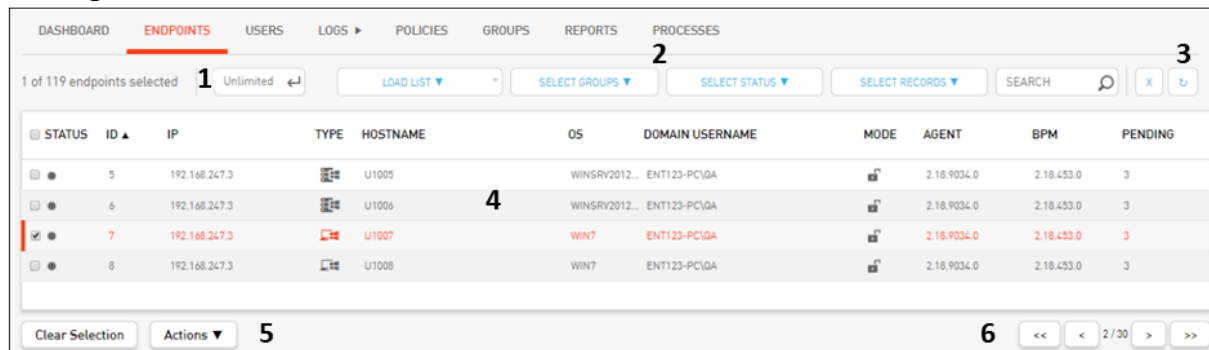
Endpoint Management Overview

The following Detection and Response Monitoring Environment components let you manage the endpoints connected to the Detection and Response server:

- **Endpoints tab:** Displays information about the endpoints and enables you to perform actions such as adding them to Groups. For more information, refer to [Viewing the Endpoints List](#).
- **Modify Endpoint Settings button:** Allows you to select the default baseline settings for all endpoints. For details, refer to [Defining Default Endpoint Settings](#).
- **Groups tab:** Allows you to manage Groups of endpoints. Endpoints in a Group can have settings that override the default endpoint settings. For more information, refer to [Endpoint Groups Overview](#).

Viewing the Endpoints List

When you select the **Endpoints** tab, a list of the endpoints currently consuming a Detection and Response Server license is displayed. The main features of the tab are described in the table below the diagram.



Number	Feature	Description
1	Limit records	Controls the length of the Endpoints list. To limit the number of endpoints included in the list, enter the desired maximum number in the field, and then click the arrow (or press <Enter>). When the Limit Records feature is in use, the word limited appears at the top of the list.

DASHBOARD

ENDPOINTS

USERS

LOGS ▶

1-7 of 50 endpoints **(limited)**



Limit records: 50



Note: Filters selected while the Limit Records feature is in use are applied to the entire Endpoints list (not only to the limited list).

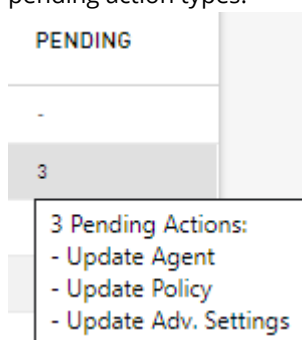
Number	Feature	Description
2	Search bar	Provides a variety of filtering options to help you find specific endpoints. For more information, refer to Filtering the Endpoints List .
3	Refresh button	Click to update the Endpoints list with the latest information from the server.
4	Endpoints grid	Lists basic information about each endpoint . Clicking any row in the grid opens a popup listing more detailed information about that endpoint .
5	Clear Selection button and Actions menu	These features appear only when the checkbox (at the left side of the grid) of at least one endpoint is selected. <ul style="list-style-type: none"> Clicking Clear Selection clears all selected checkboxes. Clicking Actions opens a list of operations that you can perform on the selected endpoint(s). For more information, refer to Performing Actions on Endpoints.
6	Navigation bar	Allows you to quickly navigate to the first, previous, next or last page of a multi-page Endpoints list.

Understanding the Endpoints Grid

The Endpoints grid provides the following basic information about each endpoint listed:

Column	Description/Notes
Status icon	Indicates the connection state of the endpoint: <div>  The endpoint is online and the Detection and Response Agent is reporting to the server.  The endpoint is disconnected from the server, or the Agent is disabled. </div> <p>This can occur when the machine is offline, or when the Detection and Response Agent is down.</p>
ID	A unique identifier associated with an approved endpoint (an endpoint that has a license to run and complies with Detection and Response Server policies). Note: If an endpoint is not yet approved, the endpoint will have a Pending status instead of an ID number.
IP	IP address of the endpoint.
Type	Category of the endpoint (workstation or server).
Hostname	Hostname of the endpoint.
OS	Operating system of the endpoint.

Column	Description/Notes
Domain Username	Details of the user logged into the domain user account.
Mode	<ul style="list-style-type: none">  Prevention Mode: The Agent detects malicious activities, blocks them, and reports them to the Detection and Response Server.  Detection Mode: The Agent detects malicious activities and reports them to the Detection and Response Server, but does not stop the activities from occurring.
Agent	The version of the Detection and Response Agent currently installed on the endpoint.
BPM	The version of the Behavioral Pattern Map package currently installed on the endpoint.
Pending	<p>Number of management actions to be carried out on the endpoint. There are four types of pending actions:</p> <ul style="list-style-type: none"> Update Adv. Settings: Updates to settings that define how the Agent behaves on the endpoint. (For details, refer to Selecting Endpoint Global Settings.) Update BPM: Updates to BPM version for the endpoint. Update Agent: Updates to Agent version for the endpoint. Update Policy: Updates to Exceptions that affect the endpoint. <p>Hovering over the number in the Pending column displays a tooltip listing the relevant pending action types.</p>



By default, the grid is sorted according to endpoint ID, in ascending order. However, you may sort the list according to any column (in ascending or descending order) by clicking the relevant column header.

Viewing Detailed Endpoint Information

Clicking a row in the Endpoints grid opens the **Endpoint Details** popup, which displays additional (read-only) data about the selected endpoint, such as:

- Latest update times
- Groups to which the endpoint belongs

- **Target Agent/Target BPM:** Indicates an updated version that is different from the currently installed one
- **Last Log:** The most recent date and time when Agent log files were sent from the endpoint to the server. Clicking the link will download the log file. If no log files have been uploaded to the server, the value will be **N/A**.

Note

You can upload files to the server from the Detection and Response Monitoring Environment using the Update Log function. For details, refer to [Performing Actions on Endpoints](#).

Property	Value
Status:	Agent - Online
ID:	49
IP:	172.21.1.158
Endpoint Type:	Workstation
Hostname:	SHAIG-LPT
Domain Username:	NYOTRON\Shai
OS:	Win10
Architecture:	amd64
Agent:	2.18.8967.2
Target Agent:	2.18.8967.2
Last Agent Update:	2017-12-25 14:40:45
BPM:	2.18.449.0
Target BPM:	2.18.449.0
Last BPM Update:	2017-12-19 17:12:17
Last Policy Update:	2017-12-21 17:57:07
Last Whitelist Update:	2017-12-25 14:40:48
Last Log:	2017-12-14 13:52
Groups:	BETA_TESTERS

Filtering the Endpoints List

The filtering options above the Endpoints list enable you to search for an endpoint, or a set of endpoints, according to a variety of criteria. The filtering options can be combined to define very specific search criteria, as required.

DASHBOARD

ENDPOINTS

USERS

LOGS

POLICIES

GROUPS

REPORTS

PROCESSES

1 of 119 endpoints selected

Unlimited

LOAD LIST

SELECT GROUPS

SELECT STATUS

SELECT RECORDS

SEARCH

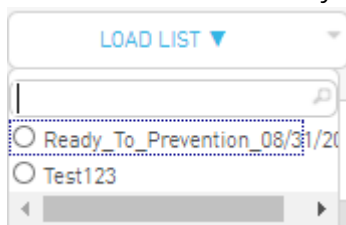
X

STATUS	ID	IP	TYPE	HOSTNAME	OS	DOMAIN USERNAME	MODE	AGENT	BPM	PENDING
	5	192.168.247.3		U1005	WINSRV2012...	ENT123-PC\QA		2.18.9034.0	2.18.453.0	3
	6	192.168.247.3		U1006	WINSRV2012...	ENT123-PC\QA		2.18.9034.0	2.18.453.0	3
	7	192.168.247.3		U1007	WIN7	ENT123-PC\QA		2.18.9034.0	2.18.453.0	3
	8	192.168.247.3		U1008	WIN7	ENT123-PC\QA		2.18.9034.0	2.18.453.0	3

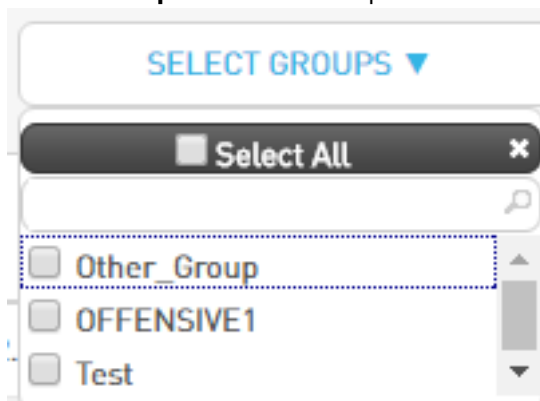
The filtering options are:

Load List: Filters according to a set of Assets that was previously selected and saved in the Detection and Response Management Console. (For more information, refer to [Viewing and Handling Assets](#).)

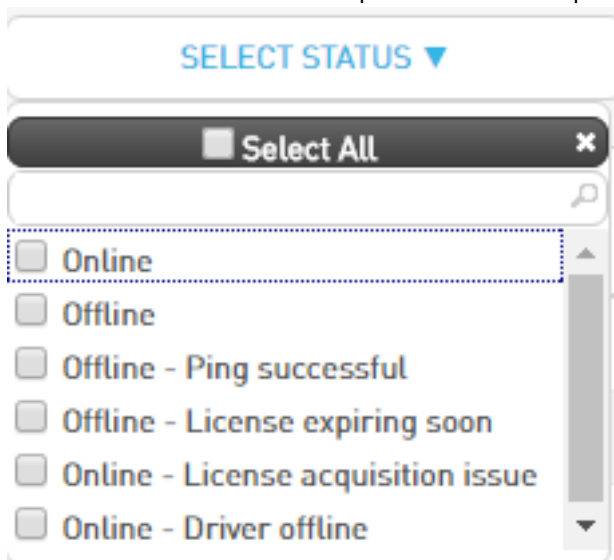
- In addition, the **Ready_To_Prevention** option enables you to view a predefined list of Assets that are ready to be switched to Prevention mode. (This list is generated daily.)



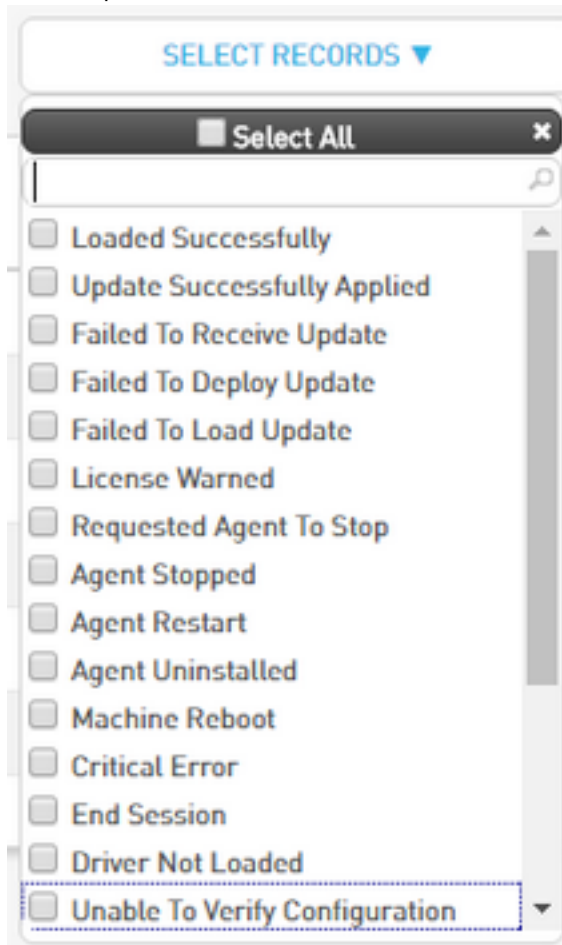
Select Groups: Filters for endpoints that belong to selected [endpoints Groups](#).



Select Status: Filters for endpoints that correspond to selected server connection statuses.



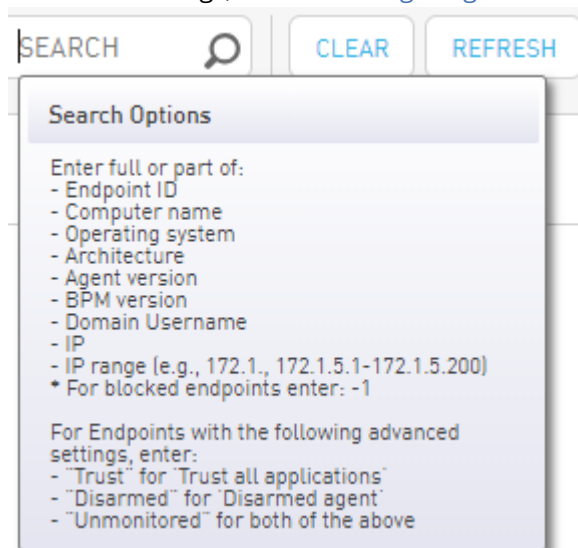
Select Records: Filters for endpoints whose Agents have sent specific messages to the Detection and Response Server.



- **Search Options:** Supports a free text keyword search according to endpoint name, IP or other identifiers.

Note


To filter according to blocked endpoints, enter **-1** in the Search field. For more information about advanced settings, refer to [Configuring Advanced Agent Settings](#).



To filter the Endpoints list:

1. To filter according to Selected Assets List, Groups, Status and/or Records, select the relevant filters from each list.

The Endpoints list is automatically filtered according to the selected options.

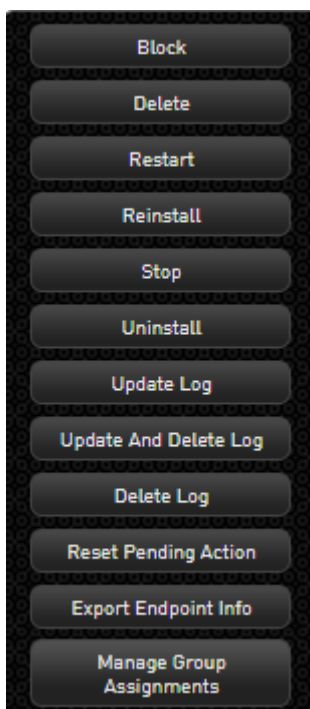
2. To perform a keyword search, enter the relevant term in the **Search** field, and then press **<Enter>** or click .

The Endpoints list is filtered according to the search term entered.

3. To clear all filtering, click **CLEAR**.

Performing Actions on Endpoints

The **Actions** button at the bottom of the **Endpoints** tab opens an options list that allows you to perform operations on a selected endpoint.



The options are:

- **Block:** Stops communication between the endpoint and the Detection and Response Server.
- **Delete:** Removes the endpoint from the list of endpoints on the **Endpoints** page. The Delete action does NOT stop communication between the endpoint and the server.
- **Restart:** Stops the Agent and immediately starts it again.
- **Reinstall:** Reinstalled Agents maintain their previous settings. You will not need to reconfigure Groups, Exceptions, etc.
- **Stop:** Deactivates the Detection and Response Agent. A stopped Agent does not monitor events on the endpoint. Stopped Agents cannot be reactivated from the Detection and Response Monitoring Environment.
- **Uninstall:** Removes the Agent from the endpoint. Endpoints uninstalled using the Detection and Response Monitoring Environment are removed from the list of endpoints on the **Endpoints** tab.
- **Update Log:** Uploads the latest log files from the endpoint to the Detection and Response Server. If an endpoint is offline when the action is selected, the log files will be uploaded when the Agent reconnects with the Server.
- **Update and Delete Log:** Retrieves the latest log files from the endpoint to the Detection and Response Server, and then deletes those files from the endpoint.

Note

After performing an Update Log action (either **Update log** or **Update and delete log**), a link for downloading the log file is displayed in the **Endpoint Details** popup of the relevant endpoint. For more details, refer to [Viewing the Endpoints List](#).

- **Delete Log:** Removes the latest log files from the endpoint (without uploading them to the Detection and Response Server).

- **Reset Pending Action:** Resets the value in the **Pending** column of the [Endpoints grid](#) to zero (in the rows of the selected endpoint(s)). The Reset action does NOT cancel the pending actions.
- **Export Endpoint Info:** Exports the information displayed in the [Endpoint Details popup](#) to CSV format.
- **Manage Group Assignments:** Enables you to control assignments of endpoints to Static Groups. For more information, refer to [Managing Static Group Assignments](#).

Managing Static Group Assignments

In order to assign Exceptions to or configure settings for an endpoint, the endpoint needs to be part of a defined [endpoints Group](#). A single endpoint can be assigned to one or more Groups.

Note

The sections below explain how to manually assign Assets to Static Groups. For information about Dynamic Group assignments, refer to [Assigning Endpoints to Groups](#).

Before beginning to handle Group assignments, open the **Groups** tab and verify that at least one Group has been defined. For details about how to add new Groups, refer to [Creating an Endpoints Group](#).

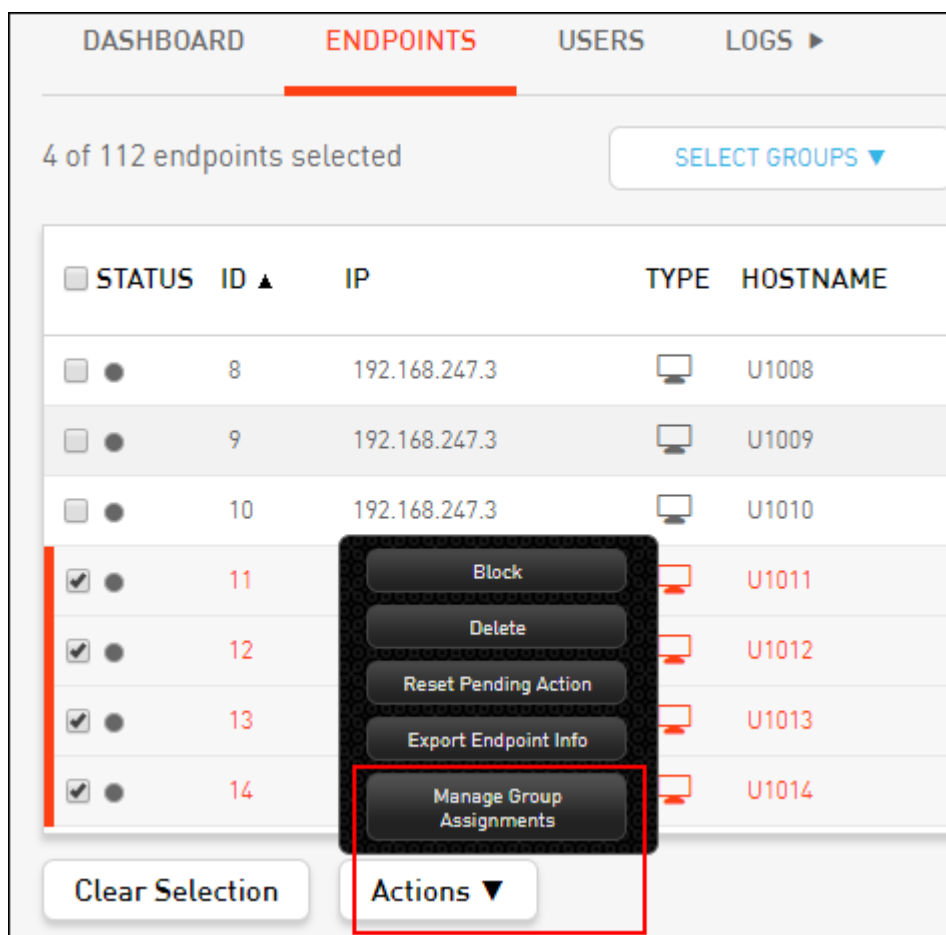
Working with the Manage Group Assignments Dialog

This dialog, which is accessed from the **Endpoints** tab of the Detection and Response Monitoring Environment, allows you to perform Group assignment actions on multiple endpoints simultaneously. For example, you can remove a set of endpoints from one Group and assign them to another Group in a single operation.

Important

The dialog is relevant for Static Groups only. Dynamic Groups are NOT listed in this dialog.

To open the **Manage Group Assignments** dialog, open the **Endpoints** tab and select the endpoints that you want to work with. Then, at the bottom of the page, click **Actions** and select **Manage Group Assignments**.



The **Manage Group Assignments** dialog has the following main portions:

- **Total selected endpoints:** The number at the upper left corner of the dialog reflects the number of endpoints you selected on the **Endpoints** tab. Any actions that you perform in the dialog will affect ALL of these endpoints, regardless of their original Groups assignments.
- **Remove From table:** This column lists the Groups to which selected endpoints are currently assigned. Keep in mind that since some selected endpoints may be assigned to more than one Group, and others may be assigned to no Groups, the total number of Affected Endpoints may be more or less than the number of selected endpoints.
To unassign the selected endpoints, select the checkbox(es) of the Group(s) from which you want to remove them. Then, click **Save**.
- **Add To table:** This column lists all defined Groups. To assign the selected endpoints, select the checkbox(es) of the Group(s) to which you want to add them. Then, click **Save**.

Note that you can move the selected endpoints from one Group to another by making selections in both tables. For details, refer to the use case example below.

Manage group Assignments

Total selected endpoints: 4

Use the table on the left to remove endpoints from Groups. Use the table on the right to add endpoints to Groups. To move endpoints from one Group to another, use both tables. Note that the specified actions will affect ALL the endpoints you selected on the Endpoints page.

Remove From:

Search

<input type="checkbox"/> Group Name	Affected Endpoint(s)
<input type="checkbox"/> Management_G...	1
<input type="checkbox"/> No_ConfidentialL...	3

Add To:

Search

<input type="checkbox"/> Group Name
<input type="checkbox"/> General_Group_Medium_Risk
<input type="checkbox"/> Management_Group_High_Risk
<input type="checkbox"/> No_Confidential_Data_Group_Low_Risk

Save

Close

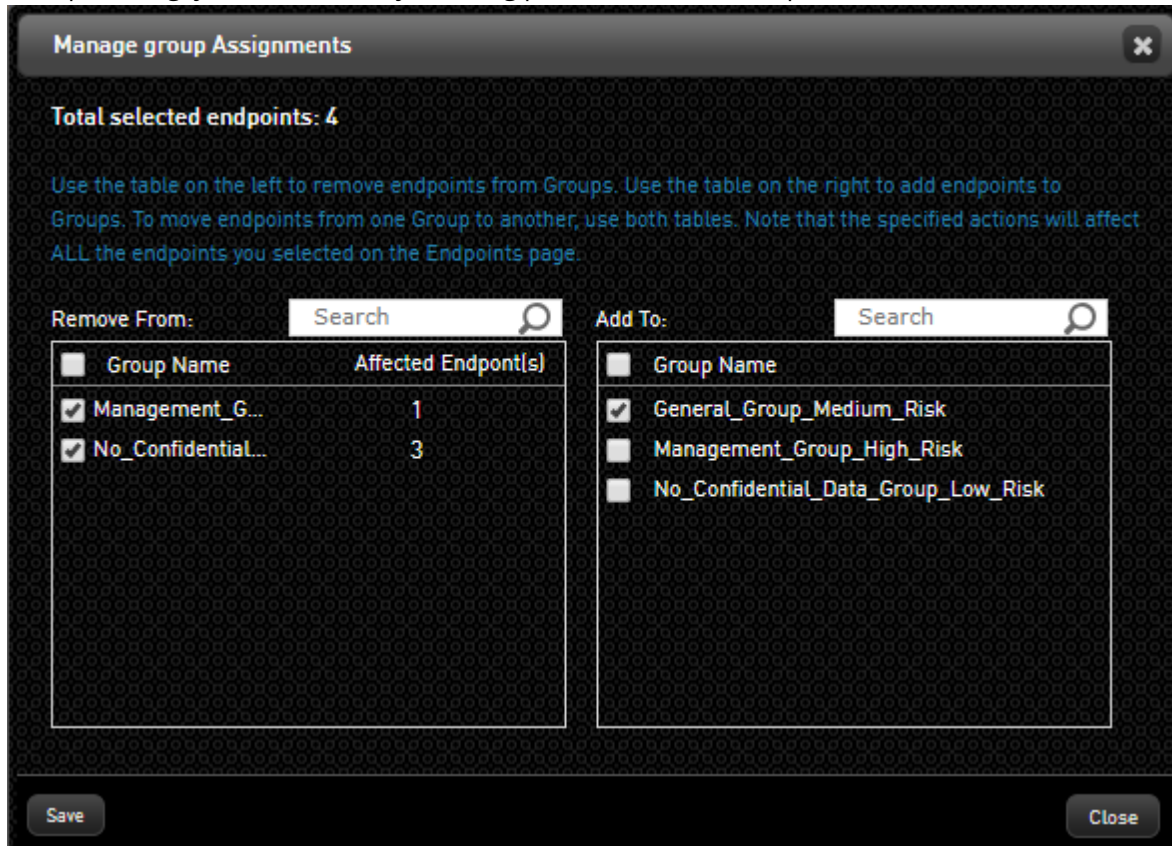
Managing Group Assignments: Use Case Example

The procedure below provides an example of how to reassign endpoints from one Static Group to another, using the **Manage Group Assignments** dialog. In our example, we will remove the four endpoints shown in the figure above from the Groups they are currently assigned to, and move them to the Group named *General_Group_Medium_Risk*.

To reassign endpoints to a different Group:

1. On the left side of the **Manage Group Assignments** dialog, select the checkboxes of the Groups from which you want to remove the endpoints. Since we want to remove the endpoints from all the Groups listed, you can select the checkbox to the left of **Group Name** to automatically select all the Groups.

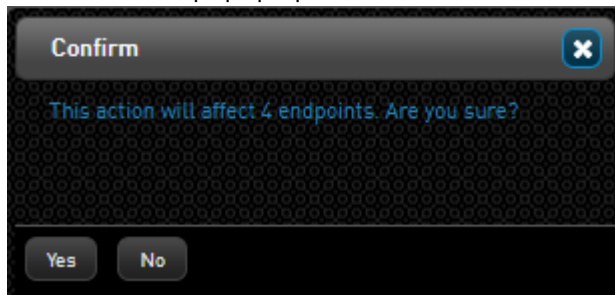
On the right side of the dialog, select the **General_Group_Medium_Risk** checkbox. (If the list of Groups is long, you can filter it by entering part or all of the Group name in the Search field.)



2.

Click **Save**.

A confirmation popup opens.

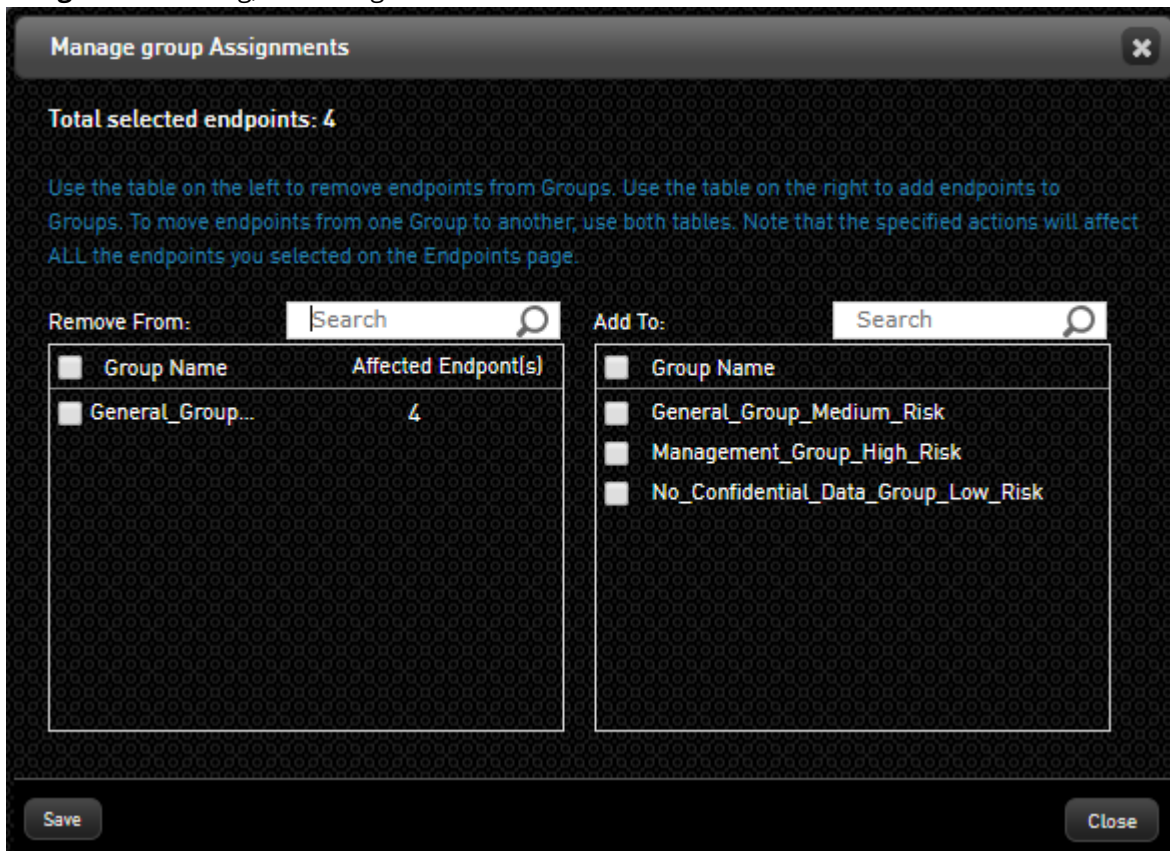


3.

4. Click **Yes**.

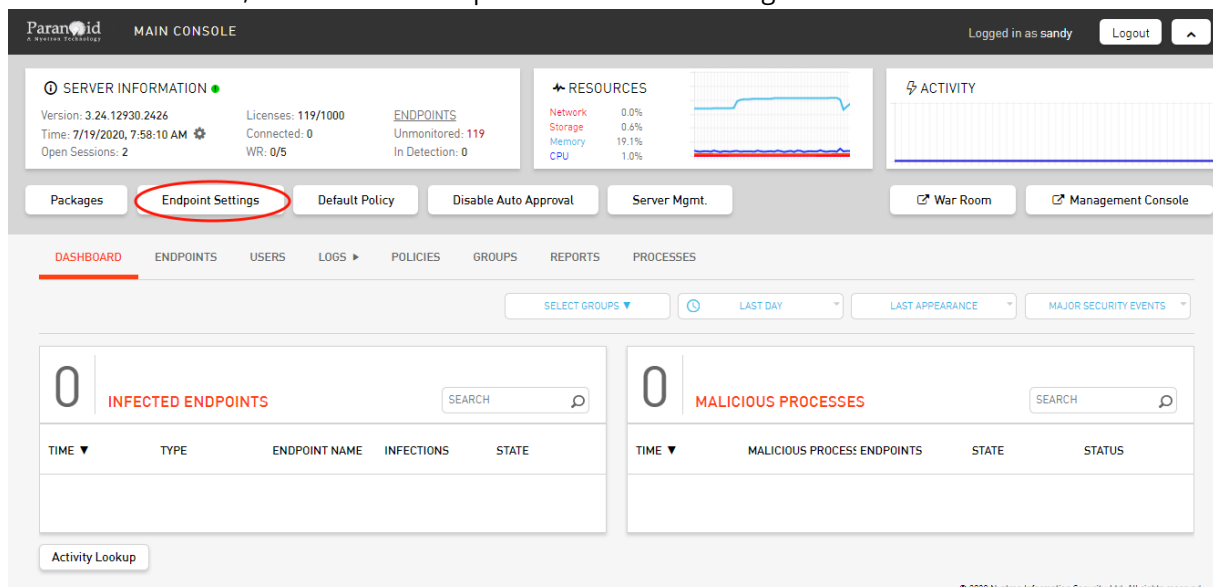
The **Manage Group Assignments** dialog closes, and the changes are saved.

If we selected the same four endpoints on the **Endpoints** tab and reopened the **Manage Group Assignments** dialog, the dialog would now look like this:



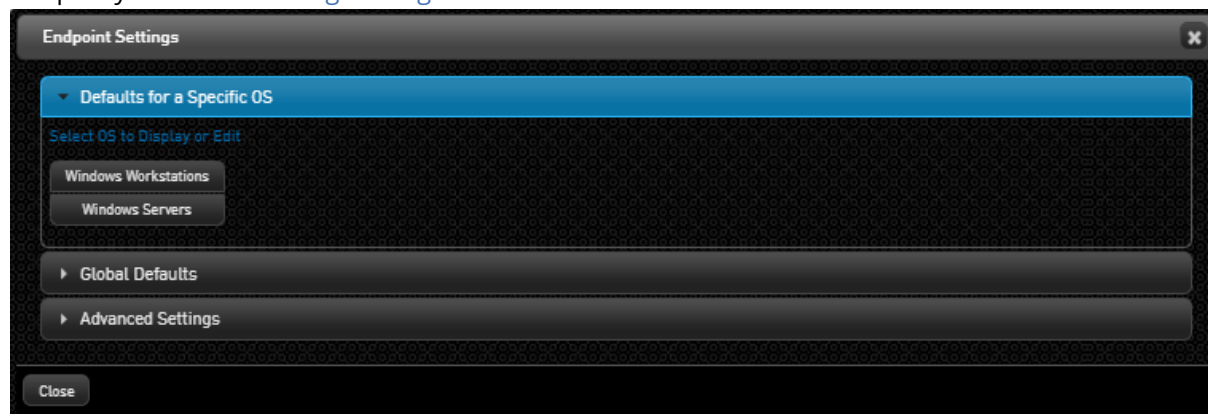
Defining Default Endpoint Settings

The **Modify Endpoint Settings** button enables you to select the default baseline settings for all endpoints connected to the Detection and Response Server. These settings include Agent / BPM versions to be used, as well as various parameters related to Agent behavior.



Clicking **Modify Endpoint Settings** opens the **Endpoint Settings** dialog. The dialog allows you to:

- Set the default Agent and BPM versions that are deployed on workstations and servers. For details, refer to [Setting Version Defaults](#).
- Select global settings for all endpoints, including Agent operation mode, the extent to which Agent activity is shared with end users, and more. For more information, refer to [Selecting Endpoint Global Settings](#).
- Specify [advanced settings for Agent behavior](#)



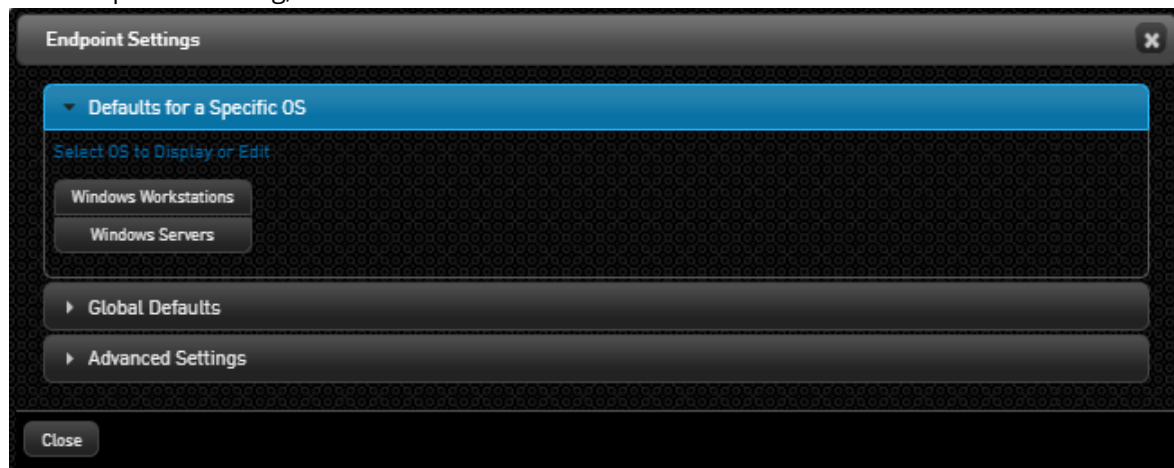
Setting Agent and BPM Default Versions

The Detection and Response Monitoring Environment allows you to set the default Agent and BPM versions for endpoints reporting to the Detection and Response Server. You can specify different default versions for workstations and servers. In runtime, each type of machine will receive the default Agent/BPM version that was selected for that type (e.g., a Windows 7 machine will get the Workstation configured version, and a Windows Server 2016 machine will get the Servers configured version). Keep in mind that Agent and BPM versions specified in Group settings take precedence over the settings selected here.

To set the default Agent and/or BPM version:

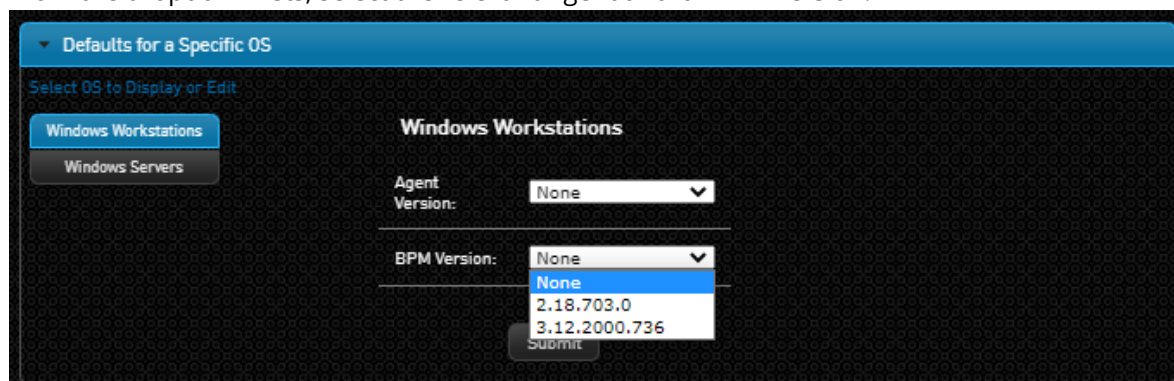
1. At the top of the Detection and Response Monitoring Environment, click **Endpoint Settings**. The **Endpoint Settings** dialog opens.

At the top of the dialog, select **Windows Workstations** or **Windows Servers**.



2.

From the dropdown lists, select the relevant Agent and/or BPM version.



3.

4. Click **Submit**.

The dialog closes, and your changes are saved in the system.

Selecting Endpoint Global Settings

The **Global Defaults** settings affect and determine certain Agent behaviors on all endpoints. You can view and update these settings by clicking **Modify Endpoint Settings** (at the top of the Detection and Response Monitoring Environment) and then opening the **Global Defaults** frame of the **Endpoint Settings** dialog.

The settings (with their default values) are described in the table below the figure. To update the settings, select the required value(s), and then click **Submit**.

Setting	Description
Customer ID	An identifier used to provide an extra layer of security for Agent-Server communication. The value is unique for each customer and is not editable.
Default Settings	<ul style="list-style-type: none"> • Popup (default = selected): When selected, a popup is presented to the end user (showing alert details) when a malicious event is prevented on endpoints. • Silent Deployment (default = selected): When selected, the installation wizard and messages are hidden during Agent installation. • Prevention (default = cleared): Determines whether the Agent works in Prevention mode. In this mode, the Agent detects malicious activities and blocks them (i.e., prevents them from occurring). In Detection mode (checkbox cleared), the Agent detects malicious activities and reports them to the Detection and Response Server, but does not stop the activities from occurring. • Detection and Response Icon (default = cleared): Determines whether or not the Detection and Response icon is visible in the system trays of the workstations. • Error Messages (default = cleared): Determines whether or not Detection and Response system error messages are displayed to end users. (Error messages may be displayed even when event popups are hidden.)
Updates	<ul style="list-style-type: none"> • Enable: All updates are sent to endpoints. • Disable: New Policy and version configurations are not sent to endpoints. However, new Agent behavior settings continue to be sent.
Tamper penalty	When the checkbox is selected, Detection and Response initiates a lockout period upon a brute-force attempt to stop the Agent. For more information, refer to Agent Tampering Protection (below).
Windows Defender Security Center Integration	When the checkbox is selected, real time scanning by Windows Defender is inactivated when Detection and Response is running.
Uninstall/Stop Secret	The secret required to locally stop or uninstall the Detection and Response Agent.

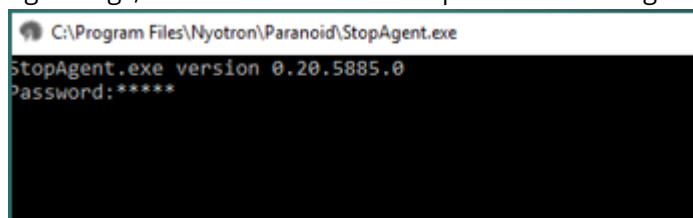
Setting	Description
Remote Mode Switch Secret	Contains the password and other settings for the Remote Mode Switch (RMS) tool, which allows the Admin to switch Agents to Disarmed or Detection mode without logging into the Detection and Response Monitoring Environment. For details, refer to Using the RMS Tool .

Agent Tampering Protection

The Detection and Response solution includes protection against AgentStop brute-force attempts. A brute-force attempt is defined as ten unsuccessful attempts to stop the Agent within ten minutes.

When the **Tamper penalty** checkbox is selected, a timeout period of ten minutes begins following a brute-force attempt. During this period, Detection and Response does not accept any password inputs (even if the password is the correct one).

Regardless of whether or not the checkbox is selected, a brute-force attempt generates alerts in the Agent logs, in the Detection and Response Monitoring Environment, and in the SIEM (if relevant).



Configuring Advanced Agent Settings

Administrative users with advanced permissions (e.g., Root users) can select settings that determine the extent of Agent endpoint monitoring, the amounts of endpoint resource consumption (e.g., memory) that trigger a warning, and more. These advanced settings are generally used in debugging and troubleshooting situations.

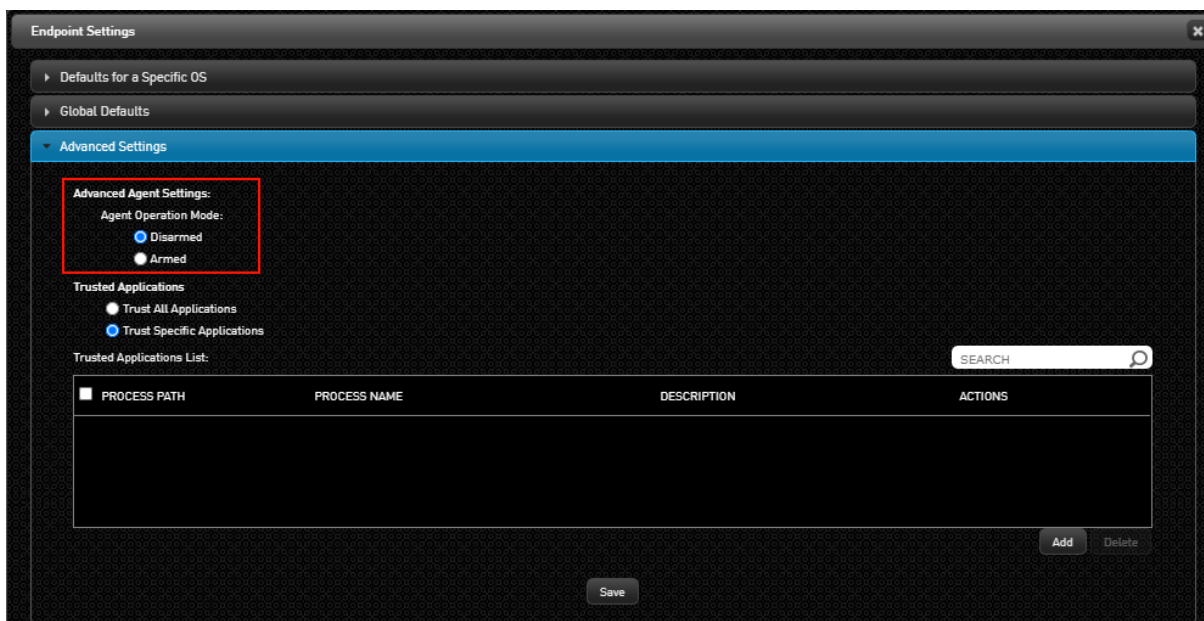
The following sections present:

- [Accessing Advanced Agent Settings](#)
- [Selecting Settings for the Armed Agent](#)

Accessing Advanced Agent Settings

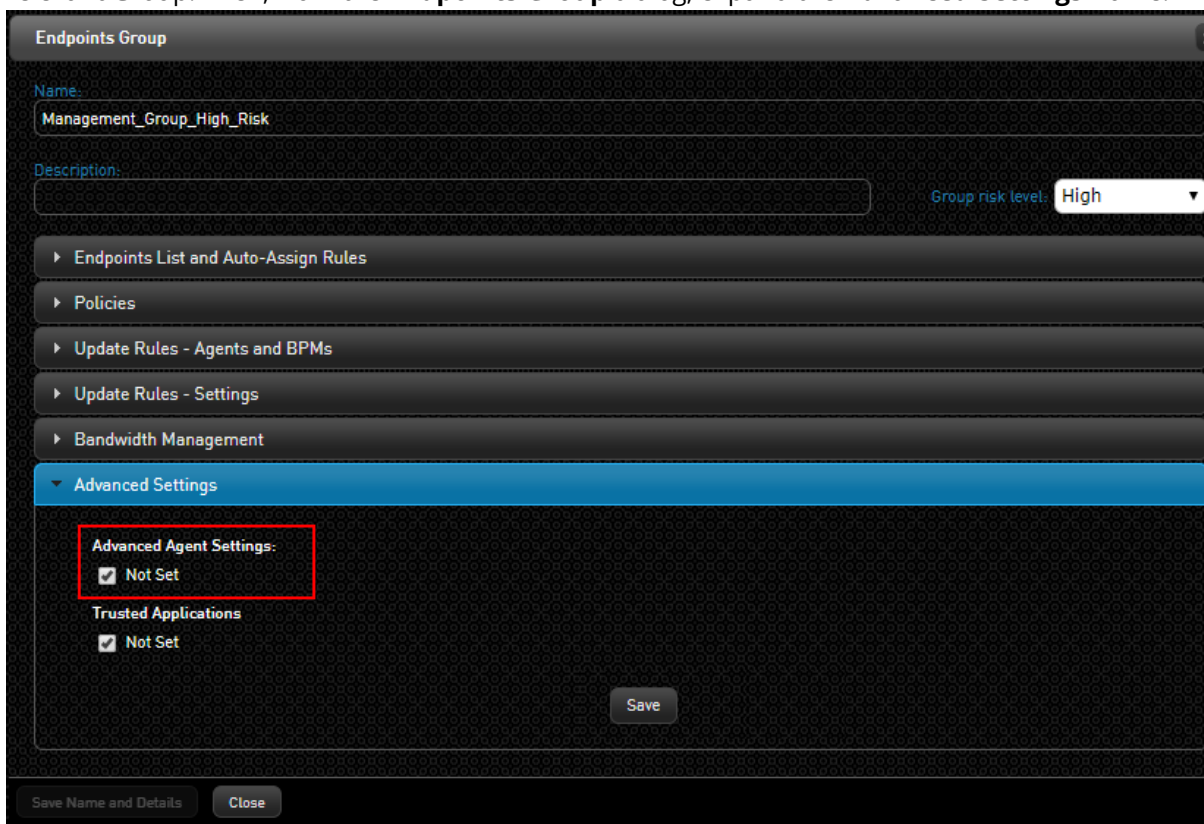
Advanced Agent settings can be specified for all Agents of the Server (global endpoint settings), or for one or more endpoint Groups. Settings defined for a Group take precedence over the global default settings.

To access advanced Agent settings for *all endpoints*, click **Endpoint Settings** (at the top of the Detection and Response Monitoring Environment console). Then, from the **Endpoint Settings** dialog, expand the **Advanced Settings** frame.



Note that by default, Agents are in **Disarmed** mode, to support a gradual Agent deployment process. Disarmed Agents maintain communication with the Detection and Response Server, but do not monitor operations on the endpoint. Disarmed Agents can be controlled remotely from the Detection and Response Monitoring Environment console.

To access advanced Agent settings for endpoints in a Group, open the **Groups** tab and select the relevant Group. Then, from the **Endpoints Group** dialog, expand the **Advanced Settings** frame.



By default, the **Not Set** checkbox is selected, indicating that no advanced Agent settings are defined for this Group. In this case, the settings are obtained from other Groups to which the endpoints are

assigned (according to Group hierarchy), or from the endpoint global settings. To view and configure advanced Agent settings, clear the **Not Set** checkbox.

Selecting Settings for the Armed Agent

Advanced Agent settings allow you to fine-tune Agent monitoring and additional parameters (e.g., the frequency at which the Agent sends statistics to the Server). In addition, they enable you to control the thresholds that trigger performance alarms.

To view the advanced Agent settings, select the **Armed** radio button. (When selecting settings for a Group, first verify that the **Not Set** checkbox is cleared.) The settings are described in the table below the figure.

Setting	Description / Notes
Performance Threshold Crossing Alarm	<p>These settings let you specify amounts of endpoint resource consumption that trigger a warning to the Server. You can change the default settings for memory, kernel memory and/or CPU.</p> <p>To update a setting, enter the threshold value for triggering an alarm. Then, in the field below, enter the number of hours for which this threshold must be consistently maintained in order to trigger the alarm.</p>

Setting	Description / Notes
Real-Time Software Installation Syncing	By default, the Agent collects certain data, such as registry keys, during installation of applications on the endpoint. To inactivate this behavior, clear the checkbox.
Statistics Sending Interval	This setting controls the frequency at which the Agent sends statistics reports (containing process information and other data) to the Server. To change the default frequency, enter the desired interval (in hours) in the field. To disable sending of statistics, enter 0 in the field.

After updating advanced Agent settings, click **Save**.

Specifying Trusted Applications

During debugging and troubleshooting, administrative users with advanced permissions (e.g., Root users) can create a list of applications defined according to file path and designate these as Trusted Applications. The Detection and Response Agent will not monitor any path that appears on the Trusted Applications List. The Trusted Applications list sent to Agents is a consolidated list of trusted applications for all Groups to which endpoints are assigned, as well as the endpoint Global Settings.

As an alternative to a Trusted Applications List, the Agent can be set to suspend all application monitoring (**Trust All Applications** setting).

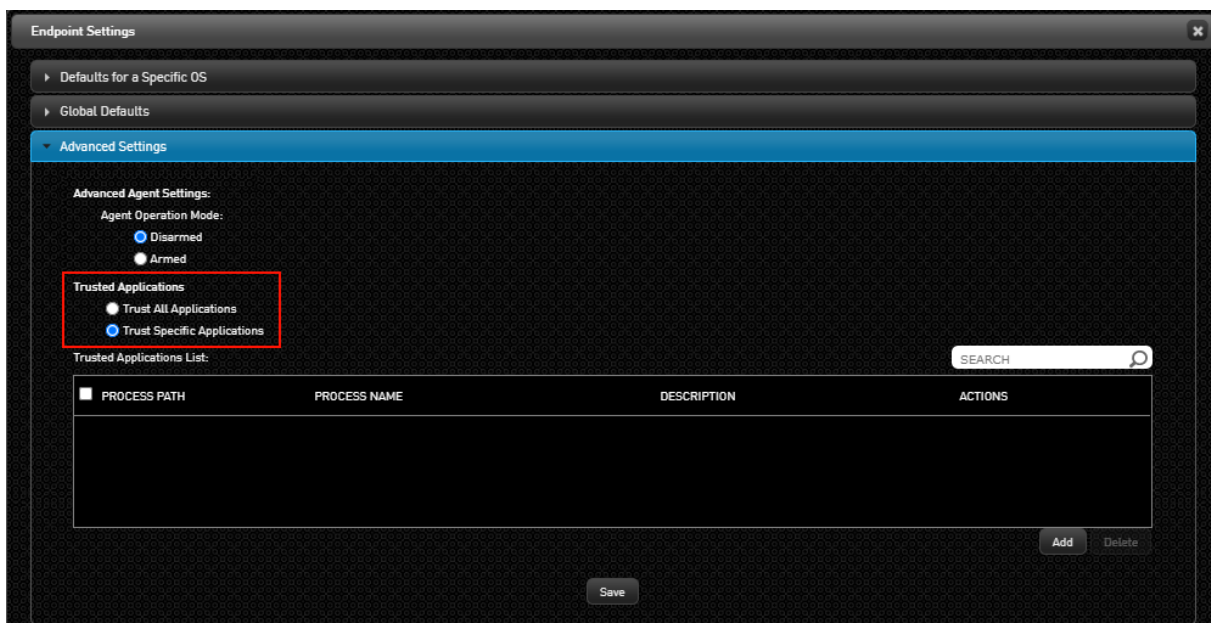
The following sections present:

- [Accessing Trusted Applications Settings](#)
- [Selecting the Trusted Applications Level](#)
- [Building and Maintaining the Trusted Applications List](#)

Accessing Trusted Applications Settings

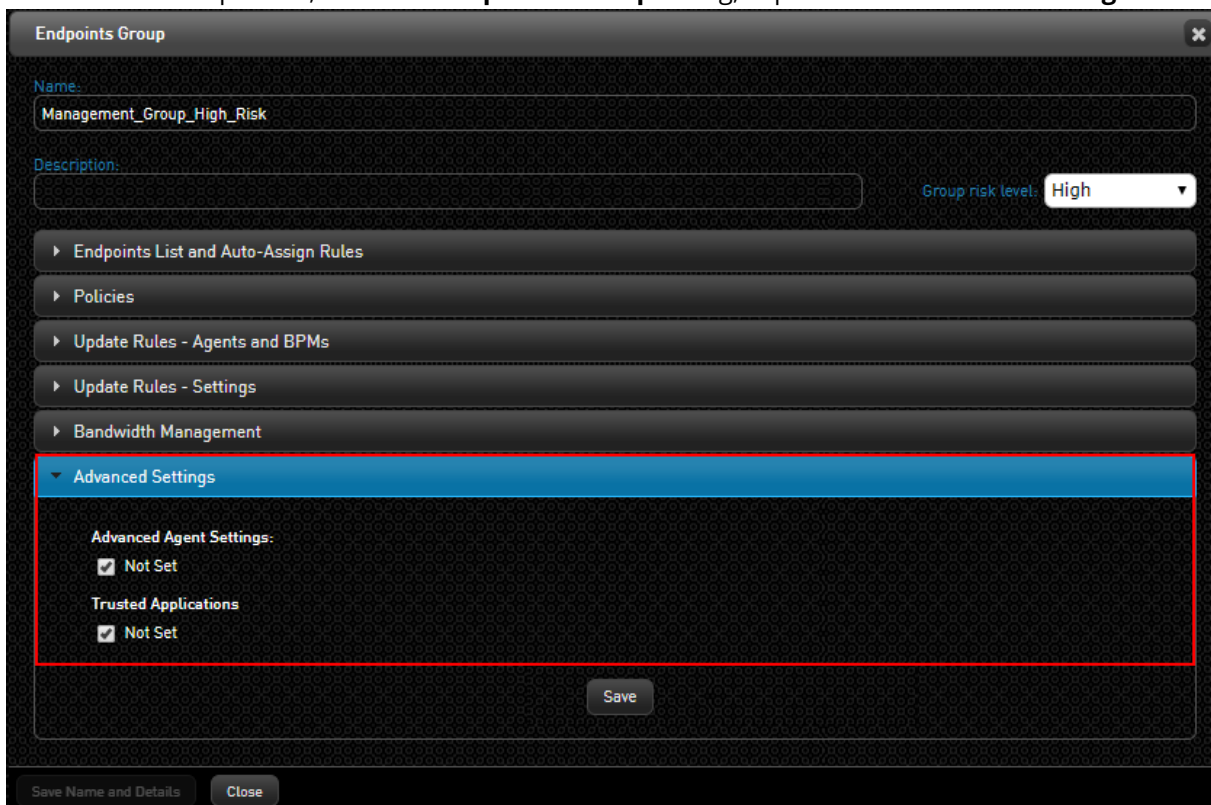
Trusted Application settings can be specified for all endpoints reporting to the Server (global endpoint settings), or for one or more endpoint Groups. Settings defined for a Group take precedence over the global default settings.

To access Trusted Applications settings for all endpoints, click **Modify Endpoint Settings** (at the top of the Detection and Response Monitoring Environment console). Then, from the **Endpoint Settings** dialog, expand the **Advanced Settings** frame.



By default, the **Trust Specific Applications** radio button is selected. For more information, refer to [Building the Trusted Applications List](#).

To access Trusted Applications settings for endpoints in a Group, open the **Groups** tab and select the relevant Group. Then, from the **Endpoints Group** dialog, expand the **Advanced Settings** frame.

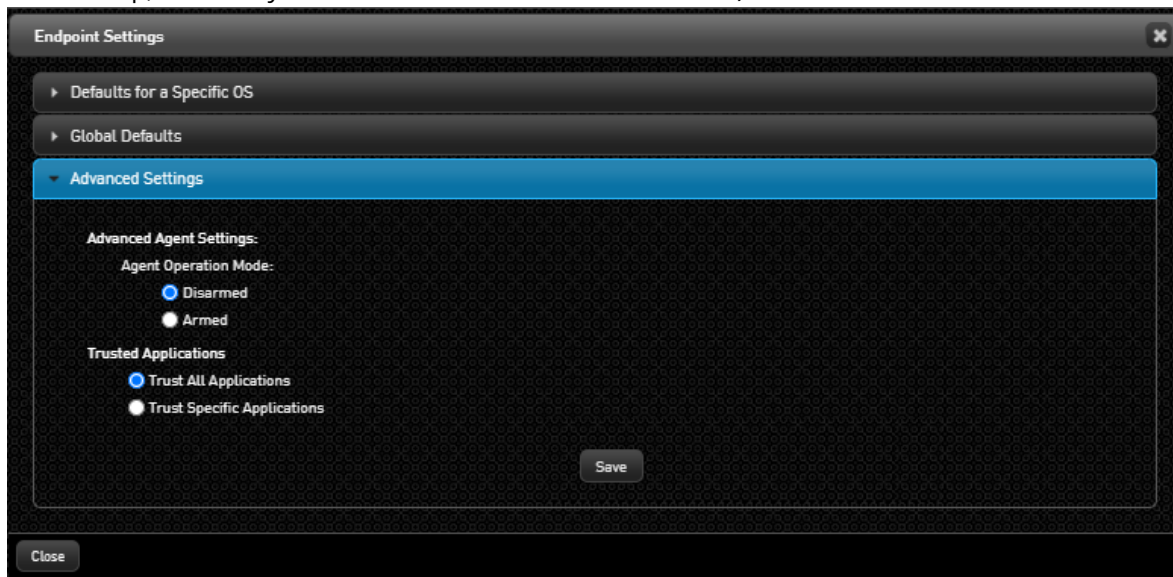


By default, the **Not Set** checkbox is selected, indicating that no Trusted Application settings are defined for this Group.

Selecting the Trusted Applications Level

When setting Trusted Applications, you can choose ONE of the following options:

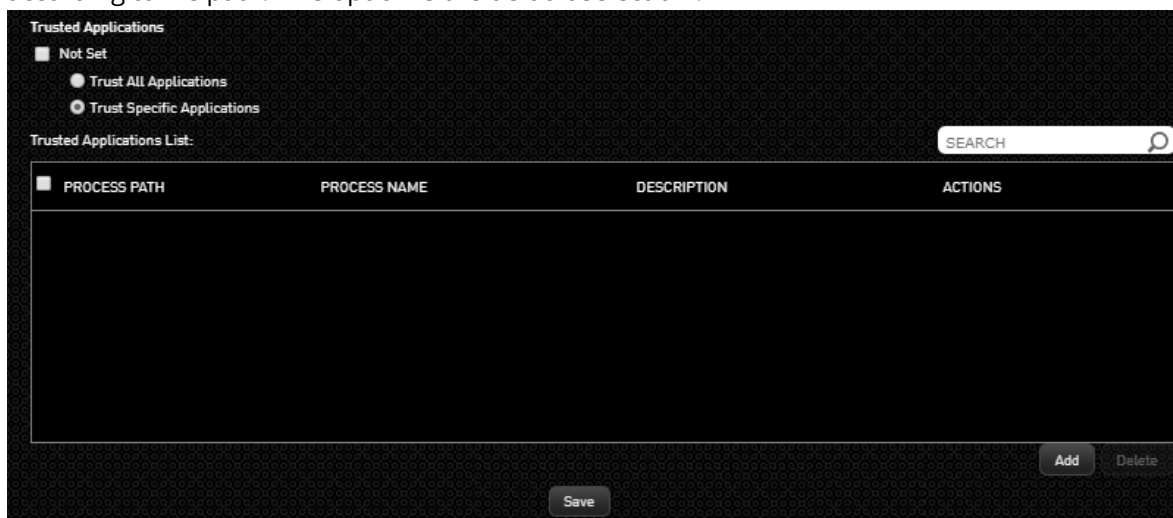
Trust All Applications: The Agent does not monitor any applications. To activate this option, select the **Trust All Applications** radio button, and then click **Save**. (When selecting this option for a Group, first verify that the **Not Set** checkbox is cleared.)



Important

Select this option for debugging and troubleshooting only.

Trust Specific Applications: The Agent does not monitor applications that are specified according to file path. This option is the default selection .



Continue by building your Trusted Applications List, as described in the next section.

Building and Maintaining the Trusted Applications List

Since Trusted Applications are defined according to path, creating the Trusted Applications List involves specifying the path of each relevant application. Once applications have been added, they can be updated and removed as necessary.

To add an application to the Trusted Applications List:

At the lower right corner of the Trusted Applications List, click **Add**.

A blank row is added to the List.

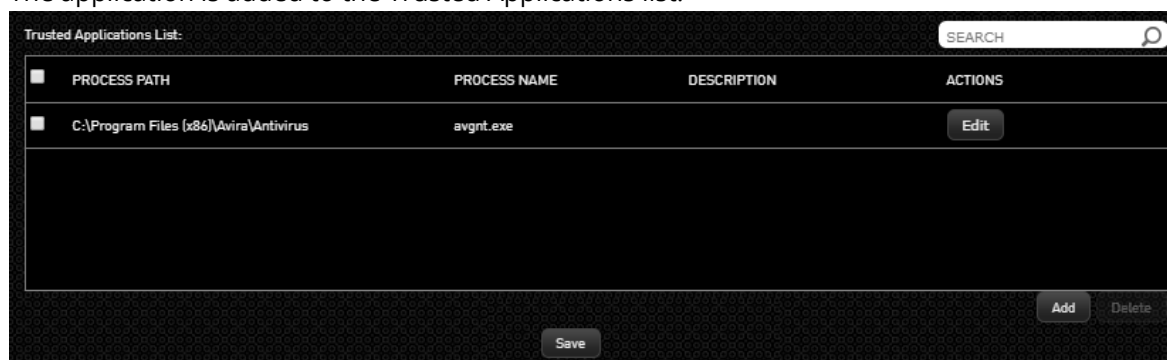


The screenshot shows the 'Trusted Applications List' window. At the top left, there are radio buttons for 'Not Set', 'Trust All Applications', and 'Trust Specific Applications'. Below this is a search bar labeled 'SEARCH'. The main area is a table with columns: 'PROCESS PATH', 'PROCESS NAME', 'DESCRIPTION', and 'ACTIONS'. A single row is present with empty input fields for the first three columns and a 'Done' button in the 'ACTIONS' column. At the bottom right, there are 'Add' and 'Delete' buttons.

- 1.
2. In the **Path** field, enter the path of the application. You may use regular expressions as necessary.
3. If there is a specific associated file that you want the Agent to avoid monitoring (e.g., an EXE file), enter the file name in the **Name** field.
4. If desired, enter a brief note in the **Description** field.

Click **Done**.

The application is added to the Trusted Applications list.



The screenshot shows the 'Trusted Applications List' window after an application has been added. The table now has one row with the following data: 'C:\Program Files (x86)\Avira\Antivirus' in the 'PROCESS PATH' column, 'avgnt.exe' in the 'PROCESS NAME' column, and an empty 'DESCRIPTION' field. The 'ACTIONS' column for this row contains an 'Edit' button. At the bottom right, there are 'Add', 'Delete', and 'Save' buttons.

- 5.
6. At the bottom of the list, click **Save**.

If there is a need to update the path, name or description of a Trusted Application, click the **Edit** button in the relevant row to make the parameters editable. After modifying the path and/or name, click **Done**, and then click **Save**.

To remove one or more applications from the Trusted Applications List, select the checkbox(es) of the relevant application(s). (Selecting the checkbox at the top, next to PATH, automatically selects all the applications.) After making your selection, click **Delete** and then click **Save**.

Using the Remote Mode-Switching (RMS) Tool

The Remote Mode-Switching (RMS) tool (**ParanoidModeSwitchingTool.exe**) allows an IT administrator to easily switch one or more Agents to Disarm or Detection mode using the Windows command line, without having to log into the Detection and Response Monitoring Environment. The RMS tool can be run locally or in a script, remotely. This tool could be useful, for instance, when there is a need to troubleshoot a potential business interruption on an Endpoint.

The RMS tool operates in both single-server and multi-server architectures. In multi-server environments, requests are sent to multiple servers in parallel. (See the section below for details.) After responses are received from the Server(s), a report is generated, summarizing the number of endpoints found and the actions taken.

Setting Up the RMS Tool

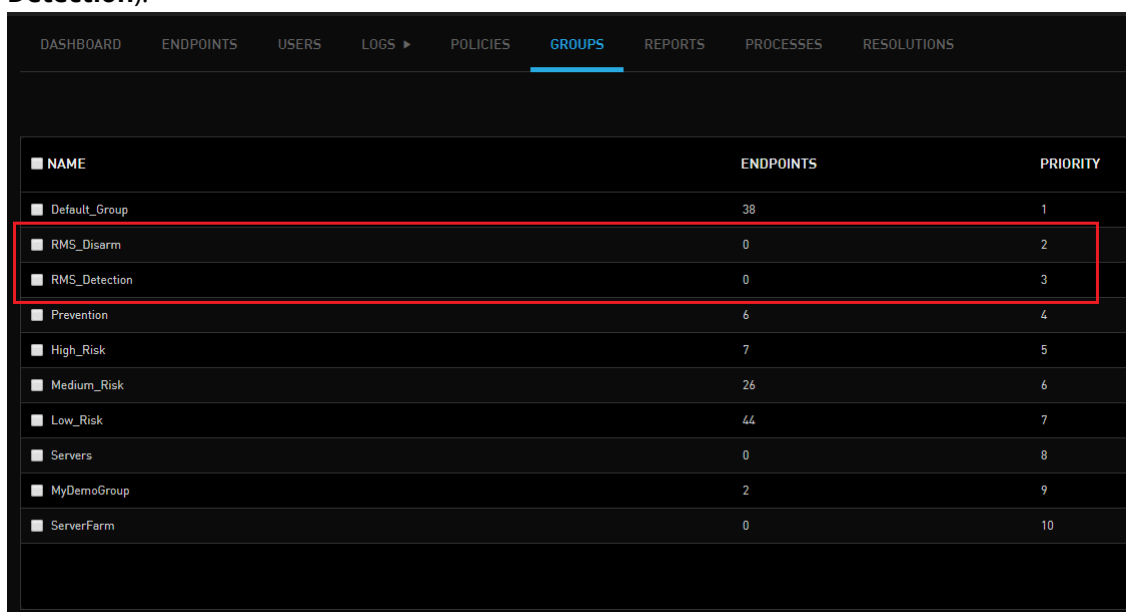
Before using the tool, the following conditions need to be met:

- You have the latest version of the RMS Tool. (To obtain the tool, contact support@acronis.com)
You have created the following two Groups in the Detection and Response Monitoring Environment:

- RMS_Disarm
- RMS_Detection

These Groups must be Static (rather than Dynamic), and have the relevant configuration (**RMS_Disarm** in Disarmed mode and **RMS_Detection** in Detection mode). The Groups are also required to have top Group priority order (priority 2 for **RMS_Disarm**, priority 3 for **RMS_**

- **Detection**).



NAME	ENDPOINTS	PRIORITY
Default_Group	38	1
RMS_Disarm	0	2
RMS_Detection	0	3
Prevention	6	4
High_Risk	7	5
Medium_Risk	26	6
Low_Risk	44	7
Servers	0	8
MyDemoGroup	2	9
ServerFarm	0	10

For more information about configuring Groups, refer to [Managing Endpoint Groups](#).

- The relevant Agents are [online in the Detection and Response Monitoring Environment](#). (If the Agents are offline, they will not receive the updates.)
- The Detection and Response Server is reachable from the host on which the tool is run. In a multi-server environment, the host must have HTTPS connectivity to all Detection and Response Servers.
- In **multi-server environments**, DNS records need to be added by creating multiple "A" records with the same name but different IP addresses, pointing to your Servers. Alternatively, you can specify multiple FQDNs or IP addresses as the *server address* parameter, in a comma-separated list.
 - Records can be created in either a public or private DNS.
 - If you wish, servers can be grouped into multiple records (e.g., you can create groups containing multiple servers based on geographical area). **All grouped servers must have the same RMS Secret** in the Detection and Response Monitoring Environment's Remote Mode Switch settings (see below).
 - The host from which the RMS tool is run must have DNS connectivity to the DNS Server where the DNS records were created.

In addition to the conditions listed above, the Remote Mode Switch settings need to be configured in the Detection and Response Monitoring Environment. These settings include password and permissions to switch to Detection, Disarm or Revert (to the original endpoint configuration). To access the settings from the Detection and Response Monitoring Environment console, select **Modify Endpoint Settings > Global Defaults**.

Running the RMS Tool

To use the RMS tool, open the Windows command prompt (**CMD.EXE**) and run the tool according to the following syntax:

```
ParanoidModeSwitchingTool /server [server(s)] /secret [secret | *] /mode [mode] /endpoints [ep1[,ep2,...,epN]] /wait [timeout]
```

Parameter	Mandatory?	Value / Notes
server	Yes	FQDN(s) or IP address(es) of the target Detection and Response Server(s).
secret	Yes	Secret phrase (password) configured on the Detection and Response Server for this tool, or * to interactively prompt for a secret (not displayed when you type it).
mode	Yes	One of: DETECTION, DISARM or REVERT. The REVERT command restores endpoints to the state that they were in before being manipulated by the RMS tool (i.e., it undoes previous DETECTION and DISARM commands).
endpoints	Yes	A comma-delimited list of endpoint names.
wait	No	<p>Add this parameter if you would like the exit code to report the actual status of the target endpoints (i.e., whether the RMS command was successfully enforced on the target Agent side). The timeout value (in minutes) is specified as part of the argument.</p> <p>When you include the <i>/wait</i> argument in your command, the RMS tool queries the server approximately every 10 seconds for endpoints that successfully enforced the RMS action. The server continues to query the endpoints until confirmation is received from all required endpoints OR until the timeout is reached.</p> <p>Note: The recommended timeout value is 10 minutes.</p>

Note

To view syntax and options, type: `ParanoidModeSwitchingTool /?`

The examples below show various use case scenarios for the RMS tool:

- Moving two endpoints to Detection mode, using the */wait* argument with a timeout of 10 minutes:
`ParanoidModeSwitchingTool /server acme-all /secret u87W24a /mode DETECTION /endpoints LAP-CENTER1,LAP-CENTER2 /wait 10`
- Moving two endpoints to Detection mode querying a multi-IP DNS record:
`ParanoidModeSwitchingTool /server acme-all /secret u87W24a /mode DETECTION /endpoints LAP-CENTER1,LAP-CENTER2`
- Moving the local endpoint to Disarm mode and prompting for secret querying two FQDNs:
`ParanoidModeSwitchingTool /server acme1.nyotron.com,acme2.nyotron.com /secret * /mode DISARM /endpoints %COMPUTERNAME%`
- Reverting two endpoints to their original configuration (REVERT) from a single server:
`ParanoidModeSwitchingTool /server acme.nyotron.com /secret u87W24a /mode REVERT /endpoints LAP-CENTER1,LAP-CENTER2`

Alternatives to Command-line Parameters

The following options can be used with the RMS tool instead of command-line parameters:

- **Configuration file:** The configuration file should be placed in the same folder as the tool, and named **ParanoidModeSwitchingTool.exe.config**. The following is an example of configuration file content:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="server" value="acme.nyotroncloud.com" />
    <add key="mode" value="detection" />
    <add key="secret" value="u87W24a" />
    <add key="endpoints" value="LAP-CENTER1,LAP-CENTER2" />
  </appSettings>
</configuration>
```

- **Environment variables:** Variables are set with the RMS_ prefix (variable names are not case sensitive). For example:

```
C:\RMS> set rms_server=acme.nyotron.com
C:\RMS> set rms_secret=u87W24a
C:\RMS> set rms_mode=disarm
C:\RMS> set rms_endpoints=LAP-CENTER1,LAP-CENTER2
C:\RMS> ParanoidModeSwitchingTool
```

RMS Tool Exit Codes

If you work with batch files / scripts, it is helpful to be familiar with the tool's exit codes:

- Exit code of **0**: Success
- Exit code **greater than 0**: Failure

For example:

```
C:\Tools\RMS Tool>start /wait ParanoidModeSwitchingTool.exe /server [REDACTED]nyotron.com /secret [REDACTED] /mode DETECTI
ON /endpoints Win10_Nyotron_E
C:\Tools\RMS Tool>echo %errorlevel%
0
C:\Tools\RMS Tool>
```

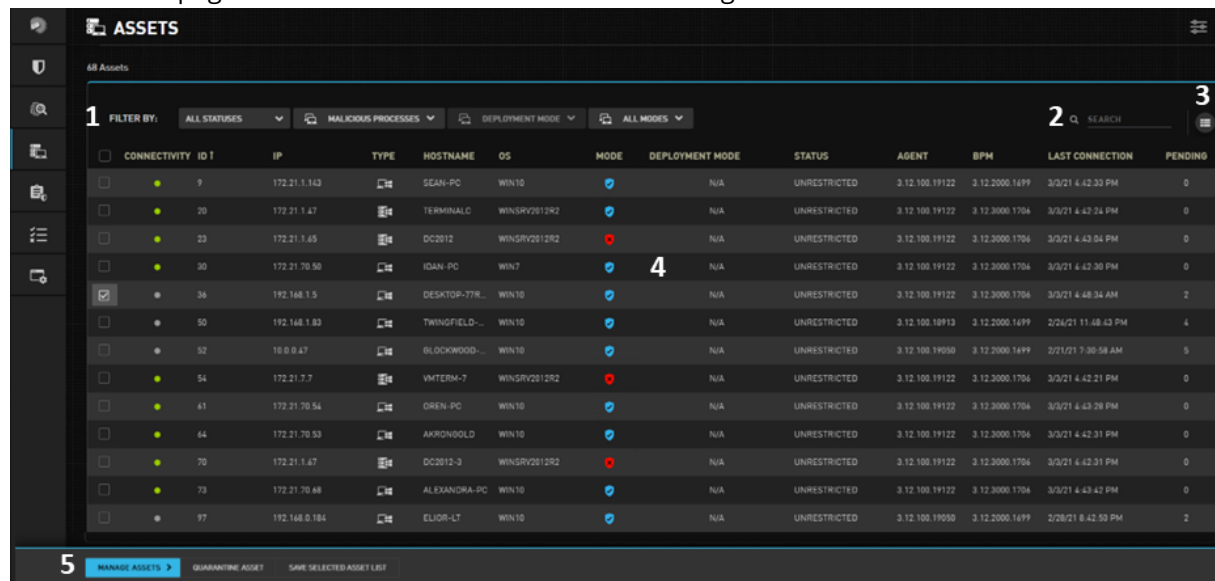
More About the RMS Tool

- The tool supports up to 1,000 endpoints in a single command-line.
- The tool reports whether actions were successful or not and displays errors when relevant (e.g., if no endpoint names were listed as required).
- Actions performed with the tool appear in the Detection and Response Monitoring Environment log (including the following information: Username, Hostname, Internal IP).

Handling Assets in the Detection and Response Management Console

Viewing the Assets List

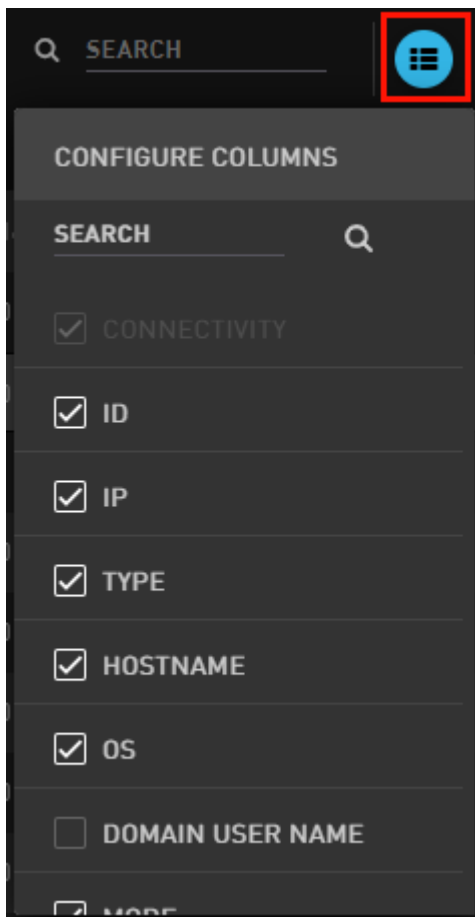
The **Assets** menu of the Detection and Response Management Console displays a list of the workstations and servers currently consuming a Detection and Response license. The main features of the **Assets** page are described in the table below the diagram.









Number	Feature	Description
1	Filters	Provide a variety of filtering options to help you find specific endpoints. For more information, refer to Filtering the Assets List .
2	Search tool	Enables you to filter the Assets list according to an entered keyword. The list is filtered as you type.
3	Configure Columns tool	Allows you to control which columns of the grid are displayed.
4	Assets grid	Lists general information about each Asset. For details, refer to Understanding the Assets Grid (below) .
5	Manage Assets actions	Allows you to perform administrative actions. For more information, refer to Performing Actions on Assets .

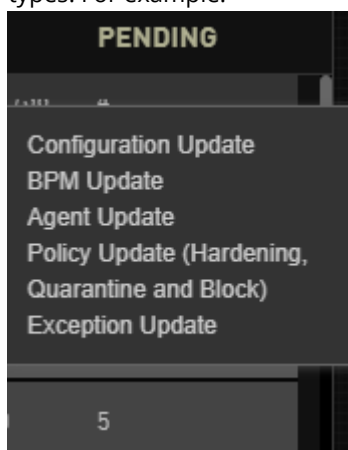
Understanding the Assets Grid

The information provided in the grid is described in the table below. You can control the column display by clicking the Configure Columns icon and selecting the columns you want to see.



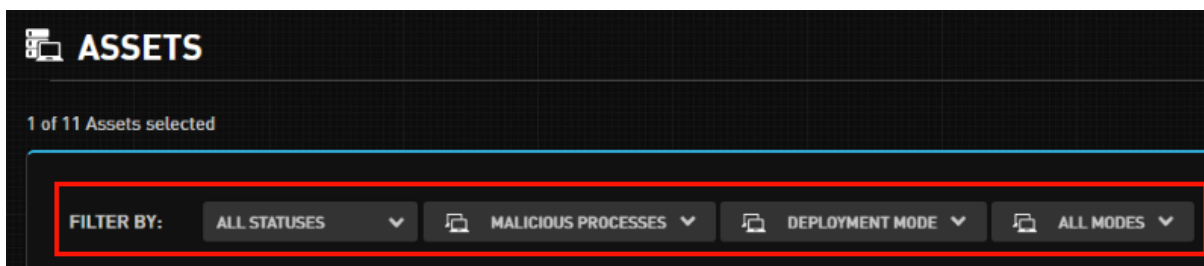
Column	Description / Notes
Connectivity	<p>The color of the icon indicates the connection state of the Asset:</p> <ul style="list-style-type: none"> : The Asset is online and the Agent is reporting to the Detection and Response server. : The Asset is disconnected from the server, or the Agent is disabled. This can occur when the machine is offline, or when the Agent is down.
ID	A unique identifier associated with an approved endpoint (an endpoint that has a license to run and complies with Detection and Response Server policies). Assets that are not yet approved have a Pending status instead of an ID number.
IP	IP address of the Asset.
Type	Category of the Asset (workstation or server).
Hostname	Hostname of the Asset.
OS	Operating system of the Asset.
Domain User Name	Details of the user logged into the domain user account.
Mode	Agent operation mode:

Column	Description / Notes
	<ul style="list-style-type: none"> •  (Prevention): The Agent detects malicious activities, blocks them, and reports them to the Detection and Response Server. •  (Detection): The Agent detects malicious activities and reports them to the Detection and Response Server, but does not stop the activities from occurring. •  : The Agent is currently Disarmed. When it is taken out of Disarmed mode, it will return to Prevention mode. •  : The Agent is currently Disarmed. When it is taken out of Disarmed mode, it will return to Detection mode.
Deployment Mode	Indicates whether Deployment Mode (a temporary stage relevant to newly deployed Assets) is still in progress or has been completed.
Status	Indicates Endpoint Protection and Response measures imposed on the Asset: <ul style="list-style-type: none"> • Quarantined: All communications to and from the Asset (with the exception of Detection and Response Server communications) are blocked. • Unrestricted: The Asset is not Quarantined.
Agent	Version of the Detection and Response Agent currently installed on the Asset.
BPM	Version of the Behavioral Pattern Mapping package currently installed on the Asset.
Last Connection	Date and time of the most recent connection to the Detection and Response Server.
Pending	Number of management updates to be carried out on the Asset. Hovering over the number in the Pending column displays a tooltip listing the relevant pending action types. For example:



Filtering the Assets List

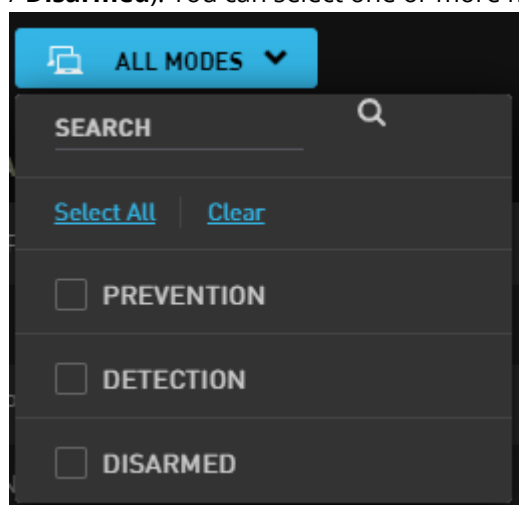
The filtering options at the top of the Assets list enable you to quickly find Assets that might be more likely to impact your organization's security status.



You can filter the list according to any or all of the following categories:

- **Asset status:** Allows you to select *one* status by which to filter the list (**Quarantined**, **Unrestricted**, etc.).
- **Malicious processes:** Allows you to filter Assets according to number and handling of malicious processes that affected them. See the procedure below for more details.
- **Deployment Mode:** Allows you to filter for Assets in Deployment Mode, Assets no longer in Deployment Mode, or both. Deployment Mode is a temporary stage following Agent installation in which Acronis's MDS analysts monitor the environment and gradually prepare Assets to work in Prevention mode. While Assets are in Deployment Mode, the Dashboard displays only security events that were prevented on them.

Mode: Allows you to filter for Assets according to Agent operation mode (**Prevention / Detection / Disarmed**). You can select one or more modes to filter by.



To use the Malicious Processes filter:

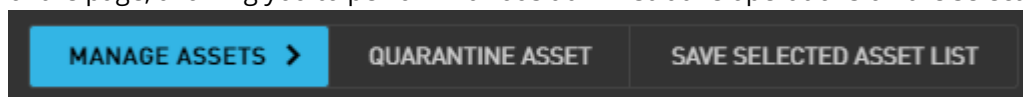
1. Click the filter to open it. Then, indicate the number of malicious process occurrences to include in the filter, by selecting the appropriate checkboxes. (You can select more than one box.)

After making your selection(s), the options below are enabled.

2. Open the **Time Frame** list and select one of the options (Last 7, 14 or 21 days).
3. Open the **Type** list and select one of the following handling options:
 - **Detected:** Some potentially malicious activities generated by the process were detected.
 - **Could Have Been Prevented:** Some or all of the malicious activities would have been prevented, had the Asset been in Prevention mode.
 - **Prevented:** The malicious activities generated by the process were blocked.
4. To begin filtering, click anywhere outside the filter frame.

Performing Actions on Assets

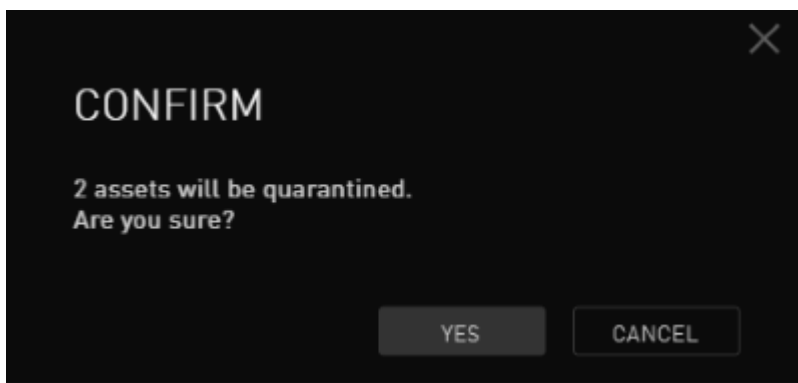
When you select one or more Assets from the Detection and Response Management Console **Assets** list (by checking their boxes), the **Manage Assets** action bar appears at the lower left corner of the page, allowing you to perform various administrative operations on the selected Asset(s).



Quarantine Asset

Quarantining an Asset blocks all communication to and from the Asset, with the exception of communications with the Detection and Response Server. Placing an infected Asset in Quarantine will prevent spread of any actual or suspected malware to other Assets in your organization.

To Quarantine selected Assets, click **Quarantine Asset**. and click **Yes** in the confirmation popup.



A message is displayed at the top of the page during the Quarantine process.



To lift the quarantine, select the Assets and click **Remove From Quarantine**.

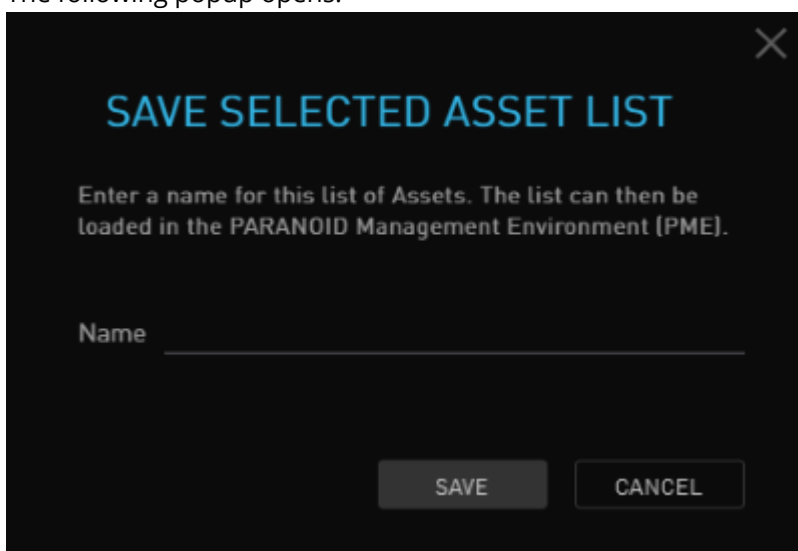
Save Selected Asset List

This action saves the Assets you select as a set of Assets that can be loaded into the **Endpoints** tab of the Detection and Response Monitoring Environment console. Once the Assets are loaded in the Detection and Response Monitoring Environment, you can assign them to Groups, retrieve their log files, perform various actions on their Agents, and more. (These actions are currently unavailable from the Detection and Response Management Console.)

To save and load a Selected Asset List:

Select the checkboxes of the Assets that you want to include in your list. Then, click **Save Selected Asset List**.

The following popup opens:



- 1.
2. Enter a name for your list, and click **Save**.
3. From the **Detection and Response Monitoring Environment**, open the **Endpoints** tab. Click **Load List** and then choose the radio button of the Selected Asset List that you want to load.

DASHBOARD

ENDPOINTS

USERS

LOGS ▶

1-4 of 119 endpoints

Unli ◀

LOAD LIST ▼

☐ STATUS


ID ▲

IP

☐ ●

1

192.168.247.3




U1001

☐ ●

2

192.168.247.3




U1002

☐ ●

3

192.168.247.3




U1003

☐ ●

4

192.168.247.3



U1004

☐ MyAssetList

☐ Test123

The Endpoints list is filtered according to the Assets in the loaded list.

Managing Endpoint Groups

Endpoint Groups: Overview

In order to configure settings for an endpoint, the endpoint needs to belong to an endpoints Group. Each Group has different settings related to [policy definitions](#), handling of update packages, and so on.

There are two different type of Groups:

- **Static:** Assets are assigned to the Group manually.
- **Dynamic:** Assets are added to and removed from the Group automatically in real time, according to Auto Assign rules.

Every Group you add must contain at least one endpoint. A single endpoint may be assigned to multiple Groups.

The following topics explain how to work with Groups:

- [Understanding the Groups Tab](#)
- [Adding and Deleting Groups](#)
- [Configuring Settings for Groups](#)
- [Assigning Endpoints to Groups](#)
- [Applying Policies to Groups](#)

Understanding the Groups Tab

The **Groups** tab displays a list of all existing endpoints Groups and provides options for managing the Groups list. The list is sorted according to [Group priority](#) (highest to lowest). Main features of the tab are described in the table below the diagram.

DASHBOARD ENDPOINTS USERS LOGS ▶ POLICIES GROUPS REPORTS PROCESSES				
SEARCH 1 🔍				
<input type="checkbox"/> NAME	ENDPOINTS	PRIORITY	3 TYPE	4 OPTIONS
<input type="checkbox"/> Default_Group	37	1	Static	Edit
<input type="checkbox"/> Prevention	6	2	Static	Edit
<input type="checkbox"/> Workstations	7	3	Dynamic	Edit
<input checked="" type="checkbox"/> High_Risk	7	4	Static	Edit
<input type="checkbox"/> Medium_Risk	26	5	Static	Edit
Add Delete Clear 5				

Number	Feature	Description
1	Search tool	Allows you to filter the Groups list according to Group name or description.

Number	Feature	Description
2	Groups grid	Displays general information about each Group, such as name, number of endpoints in the Group, and assigned priority.
3	Type	<p>Group type determines the method in which Assets are added to the Group:</p> <ul style="list-style-type: none"> • Static: Assets are added manually. For details, refer to Managing Endpoint Group Assignments. • Dynamic: Assets are added automatically according to the Auto Assign rules assigned to that Group. For more information, refer to Auto Assigning Endpoints to Dynamic Groups.
4	Options	Clicking the Edit link opens the Endpoints Group dialog, which allows you to create and modify settings for the Group .
5	Action buttons	<p>The Add and Delete buttons let you create and remove Groups. For details, refer to Adding and Deleting Groups.</p> <p>Clicking Clear unselects all Groups whose checkboxes are currently selected.</p>

Assigning Group Priority

An endpoint can be a member of several Groups simultaneously. Each Group has different settings, rules and policies. In the event that an endpoint belongs to Groups that have conflicting settings, the endpoint behaves according to the settings of the Group with the highest priority.

By default, Group priority is assigned in the order in which you create your Groups (i.e., the Group created most recently has lowest priority). However, you can rearrange the priority list as you wish using either of the following methods:


- Dragging and dropping the Groups into the desired priority order
- Entering the desired priority level in the **Group Priority** dialog

To assign Group priority using drag-and-drop:

1. From the Groups grid, assign the desired priority to each Group by moving the Groups into the required order using drag-and-drop.

As you drag and drop the Groups, the number in the **Priority** column of each row automatically changes.

At the bottom of the tab, the **Add** button is replaced by two new buttons: **Save** and **Revert**.

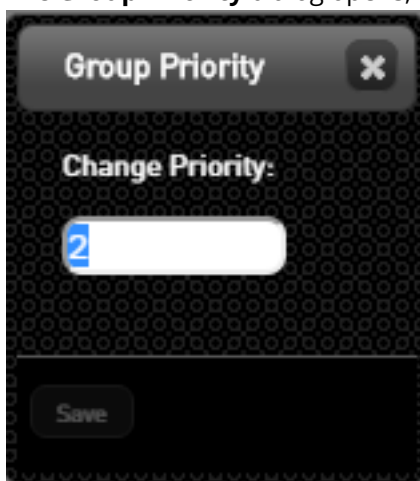
DASHBOARD ENDPOINTS USERS LOGS ► GROUPS REPORTS PROCESSES				
SEARCH 				
<input type="checkbox"/> NAME	ENDPOINTS	PRIORITY	TYPE	OPTIONS
<input type="checkbox"/> Workstations	8	3	Dynamic	Edit
<input type="checkbox"/> High_Risk	7	4	Static	Edit
<input type="checkbox"/> Medium_Risk	26	5	Static	Edit
<input type="checkbox"/> Low_Risk	44	6	Static	Edit
<input type="checkbox"/> Servers	0	7	Dynamic	Edit
<input type="checkbox"/> ServerFarm	0	8	Static	Edit
<div> <div>Save</div> <div>Revert</div> </div>				

- To apply your changes, click **Save**. Alternatively, to cancel your changes, click **Revert** .
The buttons are replaced by the **Add** button, and updates are saved in the system.

To assign Group priority using the Group Priority dialog:

From the Groups grid, in the row of the Group whose priority you want to change, click in the **Priority** column.

The **Group Priority** dialog opens, displaying the current priority of the selected Group.



The dialog box is titled "Group Priority" with a close button (X) in the top right corner. Below the title, it says "Change Priority:". There is a text input field containing the number "2". At the bottom of the dialog, there is a "Save" button.

-
- In the **Priority Level** field, enter the relevant priority level, and then click **Save**.
The **Group Priority** dialog closes. At the bottom of the **Groups** tab, the **Add** button is replaced by two new buttons: **Save** and **Revert**.
- Repeat Steps 1-2 as necessary, until all Groups are arranged in the priority of your choice.
- To apply your changes, at the bottom of the **Groups** tab, click **Save**. Alternatively, to cancel your changes, click **Revert**.
The buttons are replaced by the **Add** button, and any updates are saved in the system.

Adding and Deleting Groups

From the **Groups** tab, you can easily create new Groups, and remove Groups that are no longer in use.

Creating an Endpoints Group

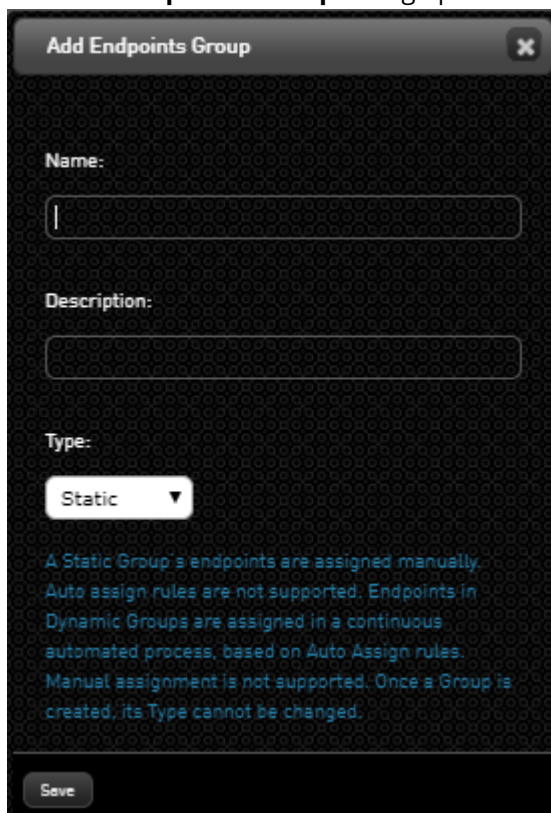
Creating a new Group involves giving the Group a name and providing an optional description. In addition, you need to specify the Group's type:

- **Static:** Assets need to be assigned to the Group manually.
- **Dynamic:** Assets are added and removed automatically in real time, according to the defined Auto Assign rules for the Group.

To create an endpoints Group:

At the lower left corner of the **Groups** tab, click **Add**.

The **Add Endpoints Group** dialog opens.



Add Endpoints Group [X]

Name:

[Text Input]

Description:

[Text Input]

Type:

Static ▼

A Static Group's endpoints are assigned manually. Auto assign rules are not supported. Endpoints in Dynamic Groups are assigned in a continuous automated process, based on Auto Assign rules. Manual assignment is not supported. Once a Group is created, its Type cannot be changed.

Save

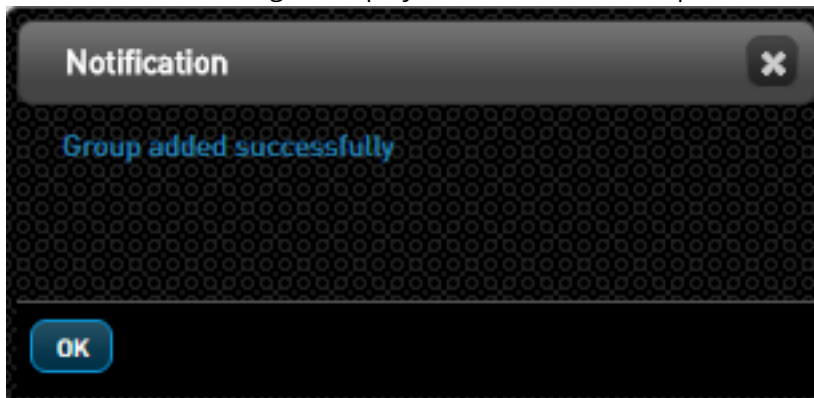
- 1.
2. In the **Name** field, enter a logical name for the new Group. The name must begin with a letter, and it may contain alphanumeric characters and underscores only. Spaces and special characters are not allowed.
3. If desired, in the **Description** field, enter a brief note about the Group.
4. From the **Type** list, select the Group type (Static or Dynamic).

Note

You will not be able to change the Group type after you create it.

Click **Save**.

A confirmation message is displayed, and the new Group is added to the end of the Groups list.



- 5.
6. Continue by assigning Assets to the new Group. For details, refer to [Managing Static Group Assignments](#) or [Auto Assigning Endpoints to Dynamic Groups](#).

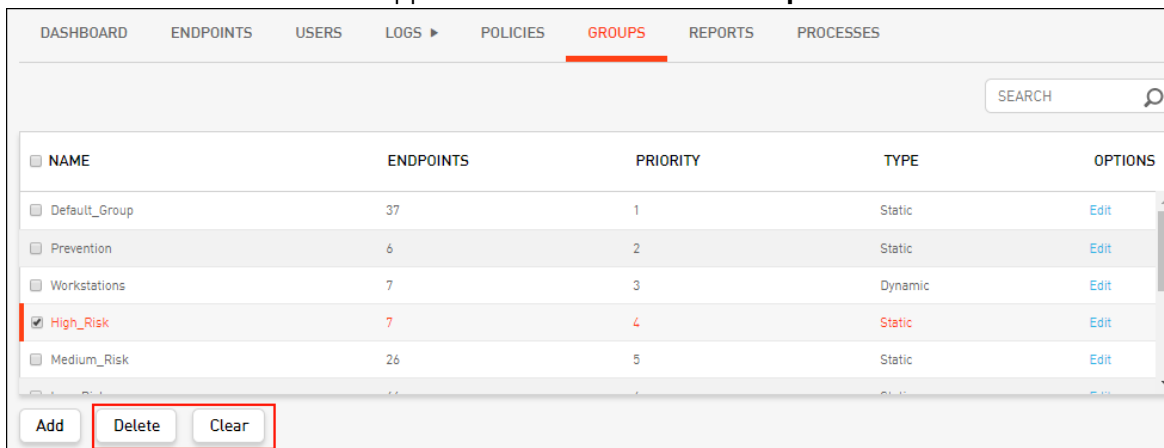
Deleting Groups

The Delete option allows you to remove Groups that are no longer necessary. You can delete several Groups simultaneously.

To delete endpoints Groups:

At the left side of the Groups list, select the checkbox(es) of the Group(s) that you want to delete.

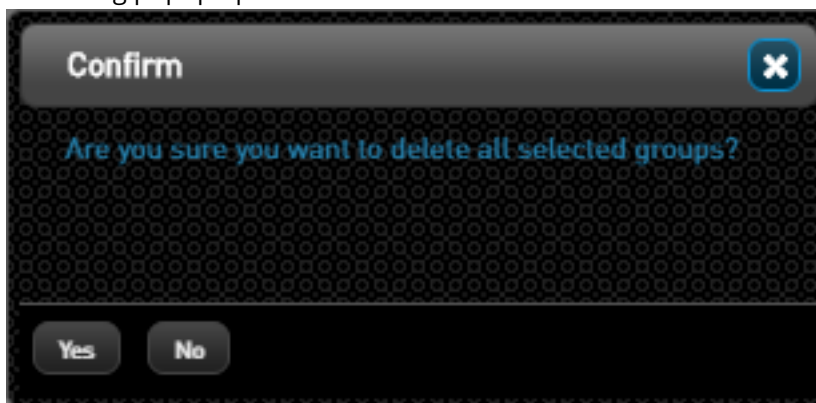
The **Delete** and **Clear** buttons appear at the bottom of the **Groups** tab.



1.

Click **Delete**.

A warning popup opens.



2.

3. Click **Yes**.

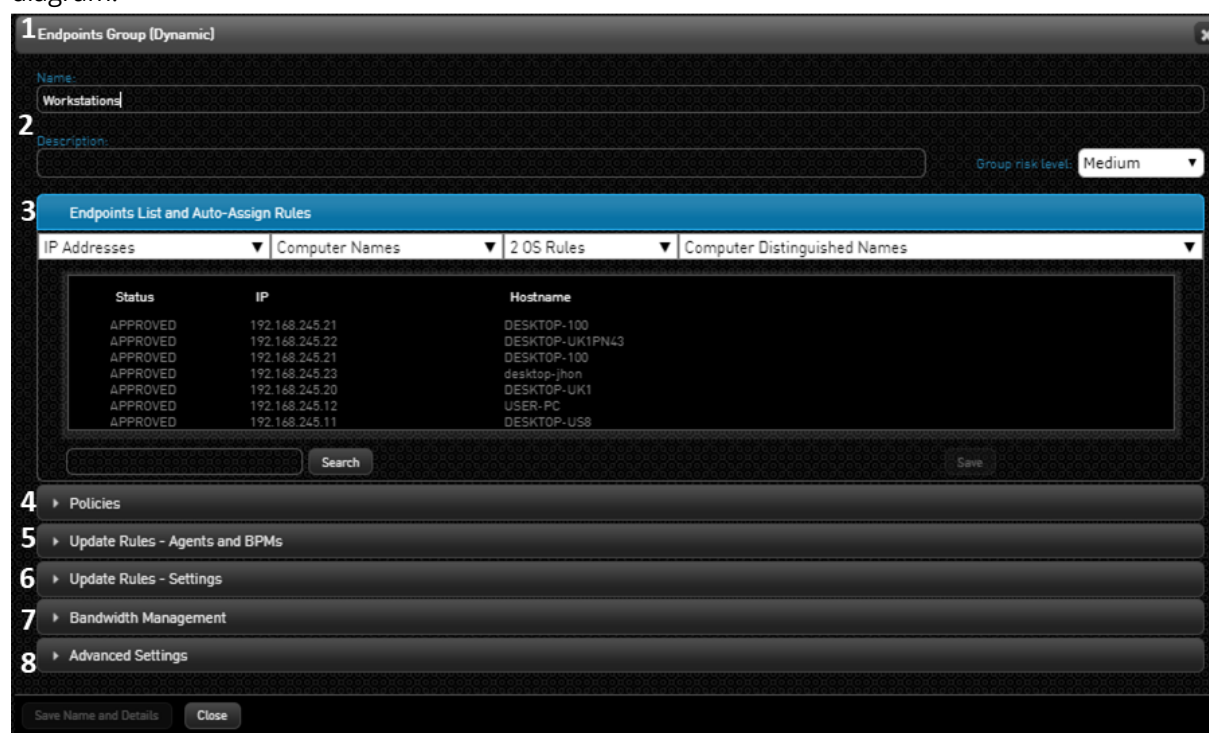
The selected Groups are removed from the Groups list.

Configuring Settings for Groups

Every endpoints Group is made up of different combinations of endpoints and controlled by different settings. The **Endpoints Group** dialog enables you to view and update the settings for a selected Group. For example, you may want to assign specific Exceptions to a Group, or set a different update procedure for some Groups.

To open the **Endpoints Group** dialog for a Group, open the **Groups** tab and click in the row of the relevant Group.

The frames and features of the **Endpoints Group** dialog are described in the table below the diagram.



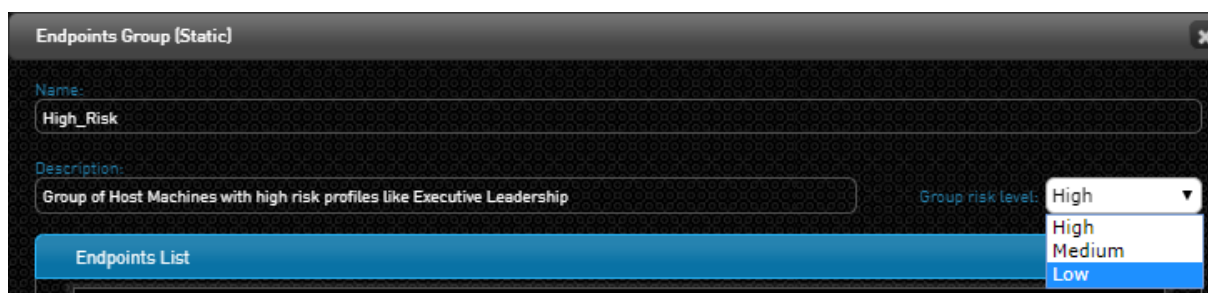
Number	Feature	Description/Notes
1	Group type	Static (Assets are assigned manually) or Dynamic (Assets are assigned automatically).
2	Name and details	Displays the Group's name, description and risk level. For information about modifying these parameters, refer to Updating Group Name and Details .
3	Endpoints List	Lists all endpoints belonging to the Group, and allows you to remove Assets from Static Groups. For details, refer to Maintaining Group Endpoints . The Auto Assign Rules (as shown in the example above) appear for Dynamic Group types only. Users with advanced permissions (e.g., Root users) are authorized to view and use the Auto Assign feature. For details, refer to #UUID-98a5882b-120c-a489-19bb-ba9a5cf1decc .
4	Policies	Enables you to assign Exceptions to the Group and manage their enforcement settings. For more information, refer to Applying Policies to Endpoint Groups .
5	Update Rules - Agents and BPMs	Enables you to select a specific Agent and/or BPM version to be installed upon update of Group endpoints. For details, refer to Selecting Update Versions .
6	Update Rules - Settings	Enables you to manage settings for Agent behavior on the endpoints in the Group. For details, refer to Selecting Agent Behavior Settings and Update Rules .
7	Bandwidth Management	Allows advanced users (e.g., Root) to define maximum upstream and downstream bandwidth rates allowed for the Group. For details, refer to Controlling Network Usage .
8	Advanced Settings	Provides advanced users (e.g., Root) with various troubleshooting options. For more information, refer to Configuring Advanced Agent Settings and Specifying Trusted Applications .

Note

All settings configured in the **Endpoints Group** dialog (except for Policies) override [global default endpoint settings](#). Endpoints in the Group are impacted by both policies in the Default Policy Set and by specific policies assigned to the Group. Policies directly assigned to the Group take precedence.

Updating Group Name and Details

The name, description and risk level of the Group can be updated as necessary. The risk level (**High**, **Medium** or **Low**) assigned is based on the value of the Group's Assets.



To update Group name and/or details:

1. At the top of the **Endpoints Group** dialog, modify the name and/or description as required by entering text in the appropriate field(s).
2. If necessary, change the risk level of the Group by selecting the relevant option from the **Group risk level** list.
3. At the lower left corner of the dialog, click **Save Name and Details**.
Changes are saved in the system.

Maintaining Group Endpoints

The **Endpoints List** frame lists all endpoints that are assigned to the Group and displays the IP, hostname, and status of each endpoint. Endpoint status can be:

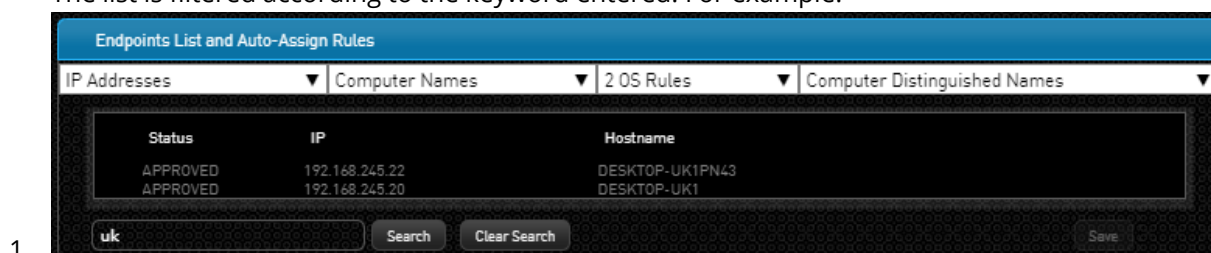
- **Approved:** The endpoint has a license to run and complies with Detection and Response Server policies.
- **Pending:** The endpoint is not yet approved.

The Search tool lets you filter the endpoints list according to a given keyword.

To filter the endpoints list:

In the Search field, enter part (or all) of the name or IP of the endpoint you are searching for. Then, click **Search**.

The list is filtered according to the keyword entered. For example:



- 1.
2. To clear filtering, click **Clear Search**.

In Static Groups (except for the Default Group), each Asset listed is preceded by a checkbox. When you select one or more checkboxes, the **Remove Selected** button appears, allowing you to unassign those Assets from the Group. For details, refer to [Assigning Endpoints to Groups](#).

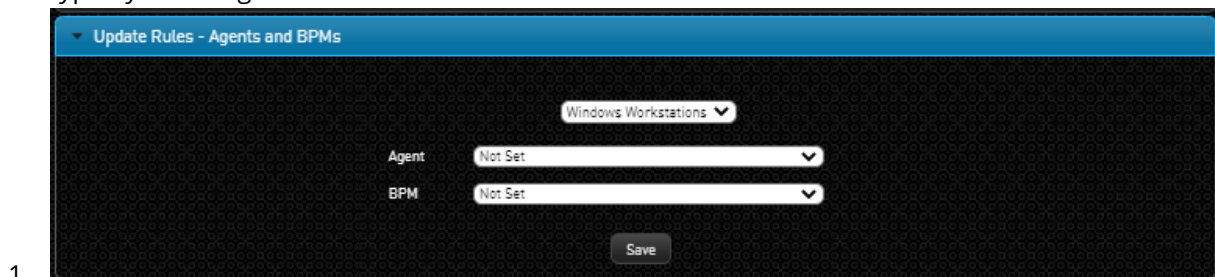
Selecting Update Versions

The **Agents and BPMs** frame of the **Endpoints Group** dialog lets you specify a BPM and Agent version with which endpoints in a specific Group should be updated. You may select different Agent and BPM versions to be deployed to workstations and servers. In runtime, each type of machine will receive the default Agent/BPM version that was selected for that type (e.g., a Windows 7 machine will get the Workstation configured version, and a Windows Server 2016 machine will get the Servers configured version).

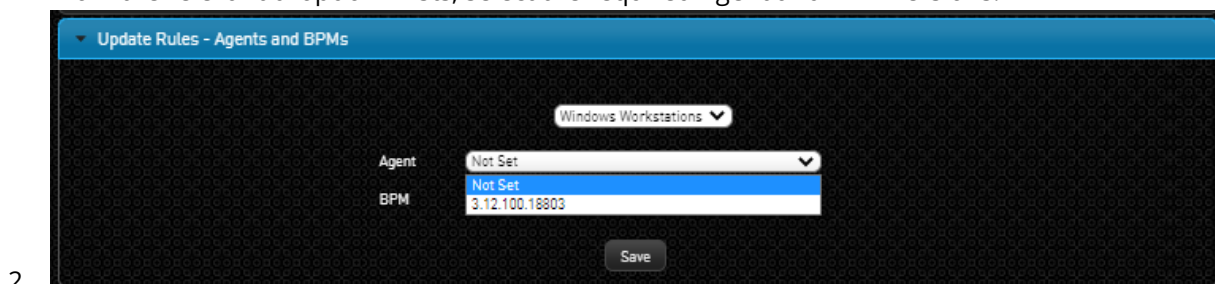
The settings specified in the **Endpoints Group** dialog override global [default endpoint settings](#).

To set the Agent and BPM version for an endpoint Group update:

At the top of the **Agents and BPMs** frame of the **Endpoints Group** dialog, specify the endpoint type by selecting **Windows Workstations** or **Windows Servers**.



From the relevant dropdown lists, select the required Agent and BPM versions.



If the **Not Set** option is selected, the version will be determined according to the default endpoint settings configured.

3. Click **Save**.

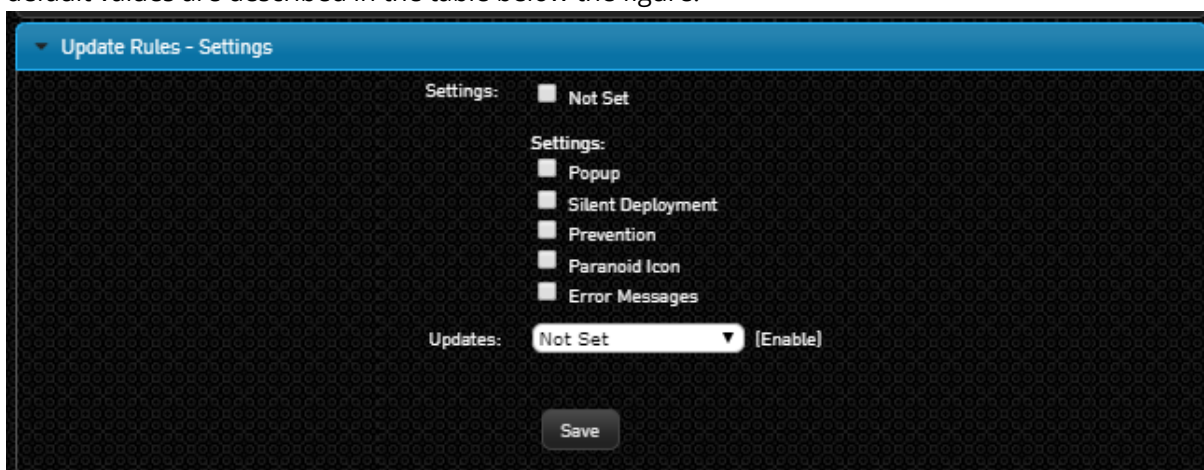
Settings are saved in the system.

Selecting Agent Behavior Settings and Update Rules

The **Settings** frame of the **Endpoints Group** dialog allows you to select settings that control Agent behavior and implementation of updates on the endpoints assigned to the Group. By default, the **Not Set** checkbox is selected, indicating that the settings are taken from a higher priority Group to which the endpoints are assigned. If there is no such Group, or if **Not Set** is selected in all Groups to which the endpoints, belong, the Global Default Settings are used.



When the **Not Set** checkbox is cleared, the settings are displayed. Agent behavior settings and their default values are described in the table below the figure.



Setting	Description	Original Default Value
Popup	When selected, a popup is presented to the end user (showing alert details) when a malicious event is prevented on endpoints.	Cleared
Silent Deployment	When selected, the installation wizard and messages are hidden during Agent installation.	Selected
Prevention	Determines whether the Agent works in Prevention mode. In this mode, the Agent detects malicious activities and blocks them (i.e., prevents them from occurring). In Detection mode (checkbox cleared), the Agent detects malicious activities and reports them to the Detection and Response Server, but does not stop the activities from occurring.	Cleared
Detection and Response Icon	Determines whether or not the Detection and Response icon is visible in the system trays of the workstations.	Cleared
Error Messages	Determines whether or not Detection and Response system error messages are displayed to end users. (Error messages may be displayed even when event popups are hidden.)	Cleared

To override default settings and update rules for an endpoints Group:

1. At the top of the **Settings** frame of the **Endpoints Group** dialog, clear the **Not Set** checkbox to display the settings.
2. Define the required settings for the Group by selecting or clearing the relevant checkboxes.

3. Specify update rules for the Group:

From the **Updates** dropdown list, select the relevant option:

- **Not Set:** Updates are sent according to the settings configured in a lower priority Group to which the endpoint is assigned. If there is no such Group, or if **Not Set** is selected for all other Groups to which the endpoint belongs, the default global setting configured for all endpoints is used.
- **Enabled:** All updates are sent to the endpoints in the Group.
- **Disabled:** New policy and version configurations are not sent. New Agent behavior settings continue to be sent to Group endpoints.

4. To save your changes, click **Save**.

Assigning Endpoints to Groups

The method of assigning endpoints to Groups varies, depending on the Group type. In Static Groups, endpoints are added to and removed from the Group manually. In Dynamic Groups, endpoints are added and removed automatically in real time, according to the [Auto Assign rules that are configured](#).

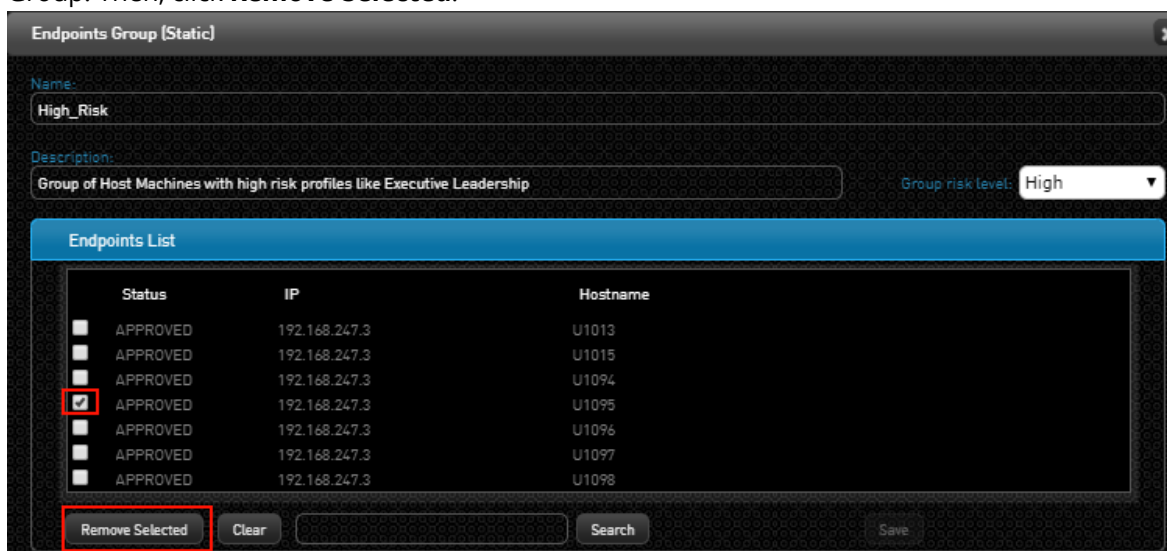
Managing Static Group Assignments

Assignments to Static Groups are controlled in the **Manage Group Assignments** dialog. This dialog allows you to perform Group assignment actions (both adding and removing) on multiple endpoints simultaneously. For more information, refer to [Managing Static Group Assignments](#).

In addition, you can remove endpoints from a Static Group directly from the **Endpoints Group** dialog.

To remove endpoints from a Static Group:

1. From the **Groups** tab, click the row of the relevant Group to open the **Endpoints Group** dialog. In the Endpoints List, select the checkbox(es) of the endpoint(s) you want to remove from the Group. Then, click **Remove Selected**.



2.

3. In the confirmation popup that opens, click **Yes**.

The selected endpoints are removed from the list, and are no longer assigned to the Group.

Configuring Auto Assign Rules for Dynamic Groups

The Auto Assign feature (available to users with advanced permissions, e.g., Root) lets you set conditions according to which Assets are automatically added to and removed from a Dynamic Group.

The Detection and Response Server continuously checks matching between Auto Assign rules and the Assets reporting to the Server, and adjusts Dynamic Group assignments accordingly. Endpoints that no longer comply with the Auto Assign rules are automatically unassigned from the Group. For example, you could create different Dynamic Groups for Assets in each regional office, with Auto Assign rules based on IP range. Roaming Agents would then be automatically unassigned from the old region's Group and added to the new region's Group, in real time.

Note

We recommend exercising caution when [configuring settings for Dynamic Groups](#). For example, it wouldn't be prudent to set an Agent version for a Dynamic Group with Auto Assign rules based on IP address, as the Agent version would be updated with each change in the IP address.

You can Auto Assign endpoints according to any or all of the following categories:

- **IP Address:** You may specify exact IP addresses, regular expressions, and/or IP address ranges.
- **Computer Name:** You can enter exact names or use *Starts with*, *Ends with*, and *Contains* expressions.
- **Operating System:** You can specify exact OS names or use *Starts with*, *Ends with*, and *Contains* expressions.
- **Computer Distinguished Name:** You can enter exact names or use *Starts with*, *Ends with* and *Contains* expressions.

The categories operate together according to *AND* logic. For example, if your conditions include JOHN-PC and WIN10, if JOHN-PC operates with WIN7 the endpoint will not be automatically assigned to the Group. However, the values within a single category (e.g., WIN7 and WIN10) operate together according to *OR* logic.

To set Auto Assign rules for a Dynamic Group:

1. From the **Groups** tab, click the row of the relevant Dynamic Group to open the **Endpoints Group** dialog.
2. At the top of the **Endpoints List and Auto Assign Rules** frame, click a category to open it. Then, enter a value in the blank row and click **+**. Refer to the tooltips for each category for format

requirements and examples.

3. Add values to each category as required. Remember that for Assets to be automatically added to the Group, they must match one of the conditions set in *each* category.

To save your settings, at the lower right corner of the **Endpoints List and Auto Assign Rules** frame, click **Save**.

The number of rules in each category appears next to the category name, and the defined rules are displayed when you click the category.

- 4.

Controlling Network Usage

To control download rates and prevent network congestion, Detection and Response supports throttled data transfer to and from the Server. Authorized administrators may specify an average total downstream bandwidth rate for data transfer to all Endpoint Groups. Maximum average bandwidth rates - for both downstream and upstream - for individual Groups can then be defined in the Group settings ([Group Bandwidth Management](#)).

Total Downstream Bandwidth Management

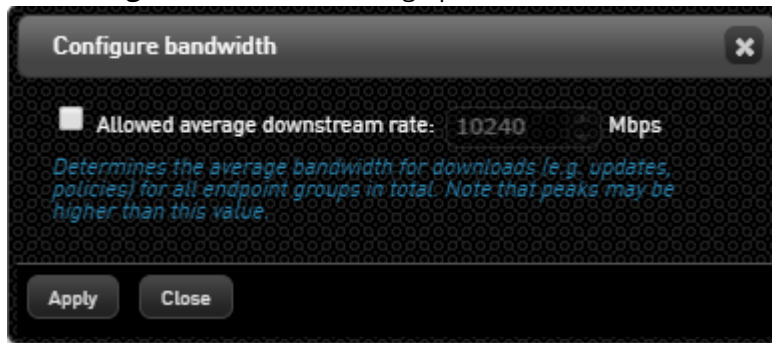
The total downstream bandwidth value is configured in the Server Management settings. This value determines the average bandwidth for downloads (updates, policies, etc.) to all Endpoints Groups. The total downstream bandwidth can then be divided among your Groups (in the Group settings) according to the requirements of each Group.

When setting the average total downstream rate, keep in mind that the value you set is the upper limit of the combined downstream rates that are set for each Group. For example, four Groups have a maximum downstream rate of 250 Mbps each (totaling 1,000 Mbps) and the total downstream rate is set at 800 Mbps. If all four Groups are receiving data transfers simultaneously, the bandwidth rate caps at 800 Mbps, and one or more of the Groups will therefore not be able to use their total allocated bandwidth.

To set the average total downstream bandwidth rate:

From the Detection and Response Monitoring Environment console, click **Server Management** and select **Configure bandwidth**.

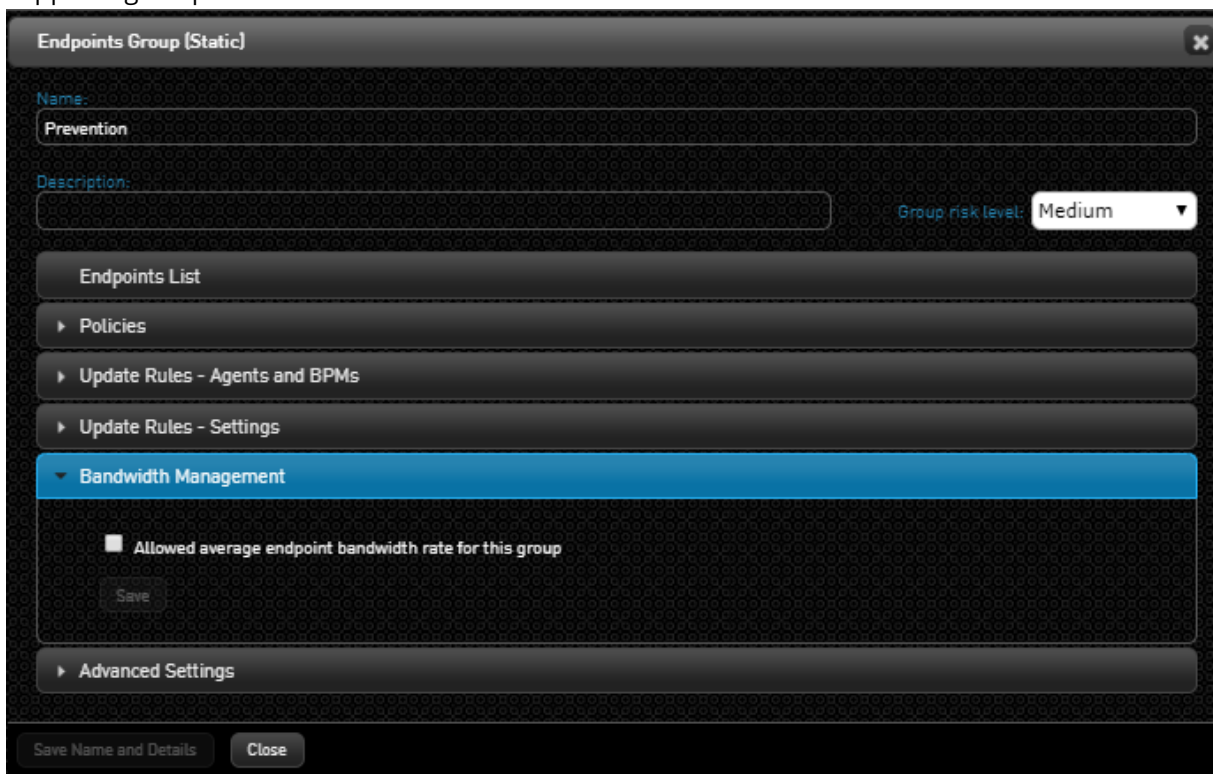
The **Configure Bandwidth** dialog opens.



- 1.
2. Select the checkbox. Then, define the allowed bandwidth rate by entering a value in the fields, or by using the Up/Down arrows to specify a value.
3. To save your changes, click **Apply**.

Group Bandwidth Management

The Bandwidth Management feature helps to prevent network congestion by allowing authorized administrators to define maximum upstream and downstream bandwidth rates that are allowed for a group. The feature is particularly useful for managing large amounts of data transfer and for supporting endpoints in areas with limited bandwidth.



To implement bandwidth management for a Group:

At the bottom of the **Endpoints Group** dialog of the relevant Group, select the checkbox in the **Bandwidth Management** frame.

Bandwidth management settings are displayed.

The screenshot shows a 'Bandwidth Management' dialog box with a blue header. Inside, there is a checked checkbox labeled 'Allowed average endpoint bandwidth rate for this group'. Below this, there are two sections: 'Upstream (e.g event reporting):' and 'Downstream (e.g updates, policy changes):'. Each section has a text input field containing the value '100' and a unit selector set to 'Mbps'. Under each input field, there is a small blue italicized note: 'The maximum upstream for this group will not exceed the above limitation.' and 'The maximum downstream for this group will not exceed the above limitation.' respectively. At the bottom left of the dialog is a 'Save' button.

- 1.
2. Define the maximum average allowed upstream and downstream bandwidth rate by entering values in the fields, or by using the Up/Down arrows to specify a value.
Keep in mind that the upstream value you set will be divided equally among all the endpoints in the Group. For example, if you allows 100 Mbps for a Group of four endpoints, each endpoint will have an upstream bandwidth rate of 25 Mbps.
3. To save your changes, click **Save**.

Analyzing Processes in the Detection and Response Monitoring Environment

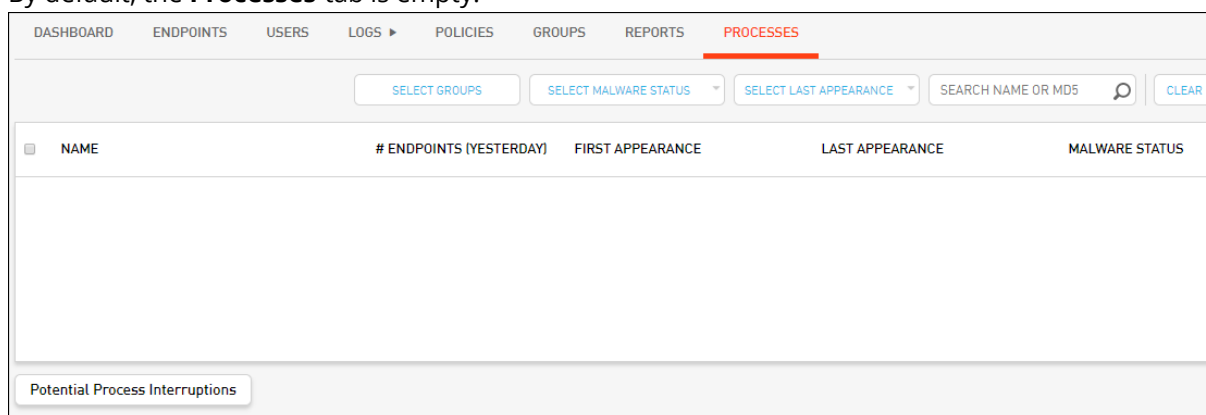
Viewing Processes in the Detection and Response Monitoring Environment

The **Processes** tab lets you view and analyze processes that are running or have run on Assets reporting to the Detection and Response Server. Any process that was monitored by the Detection and Response driver can be displayed in this tab, regardless of whether or not the process involved suspicious events that were detected/prevented by the Agent.

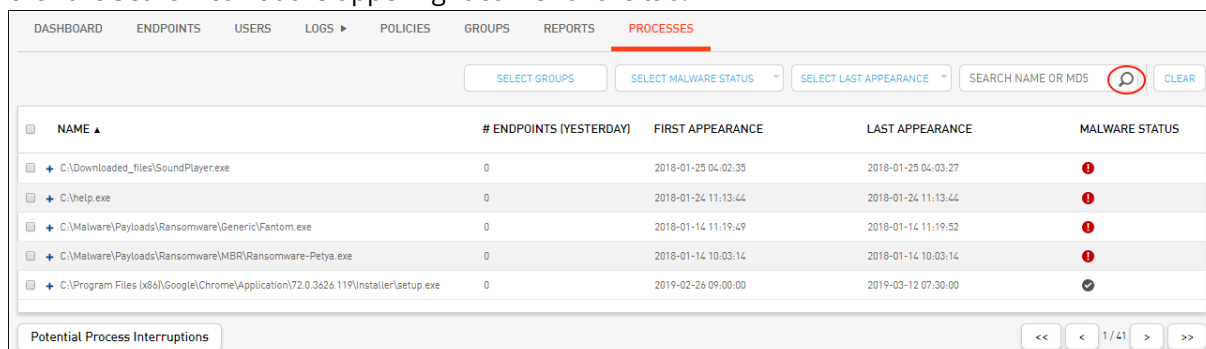
Using the **Processes** tab, you can:

- Quickly see the malware status of a process
- Search for processes according to extensive filtering criteria to easily obtain detailed information
- View lists of [potential process interruptions](#) (events that were automatically solved)

By default, the **Processes** tab is empty.




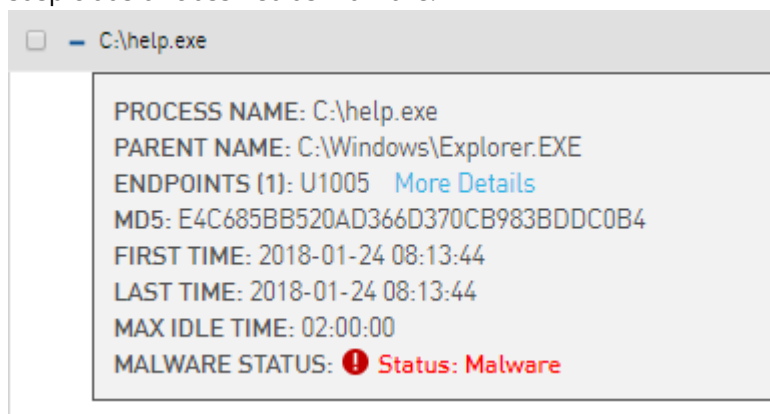
To display processes, select the [relevant filters](#). Alternatively, to populate the grid with all processes, click the Search icon at the upper right corner of the tab.



For more information about the grid columns, refer to [Understanding the Processes Tab](#).

Viewing Process Details

Clicking the  icon to the left of a process name opens a frame displaying more information about the process, such as MD5 identifier. Additional details are provided for processes that are suspicious or classified as malware.



Clicking the **More Details** link at the end of the **Endpoints** row opens an additional frame that shows detailed information about the endpoints that ran the process (if relevant).



Viewing Potential Process Interruptions

Occasionally, some detected False Positive events are automatically solved by the Server through creation of an internal Exception. Since they have been solved, these processes do not appear in the Dashboard, but they are recorded in Potential Interruptions logs. You can view or download any of these log files.

To view or download Potential Interruptions logs:

1. At the lower left corner of the **Processes** tab, click **Potential Process Interruptions**.

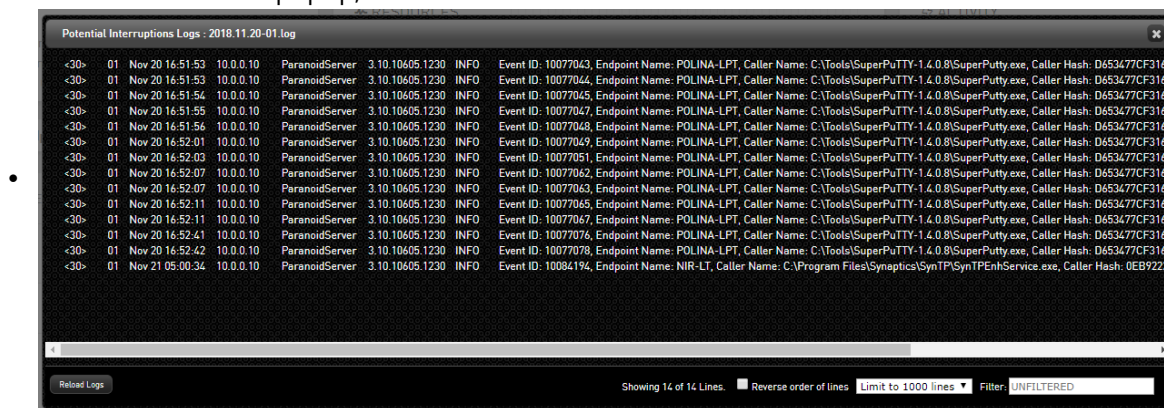
The **Potential Process Interruptions** dialog opens.



2. Open the list and select the relevant log file. (The name of the file indicates its creation date.) Then, choose one of the following options:

- To download the file, click **Download**.

To view the file in a popup, click **View**.



Understanding the Detection and Response Monitoring Environment Processes Tab

The grid in the **Processes** tab of the Detection and Response Monitoring Environment displays the following information about each process listed:




- **Name:** Full path of the process.
- **# Endpoints (Yesterday):** Number of Assets on which the process was identified during the most recent midnight to midnight 24-hour period. For example, if you are looking at the list on Wednesday at 10:00 am, the value reflects the number of Assets affected between Tuesday at 00:00 and Wednesday at 00:00.

Note

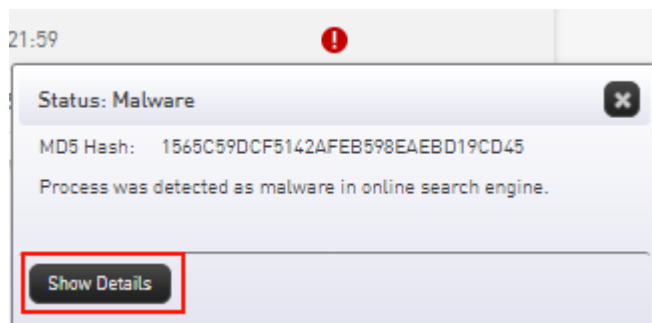
Due to the method of calculation of # Endpoints, the value in this column might not be affected by the [filters applied to the Processes list](#).

- **First Appearance:** Date and time when the process was first identified.
- **Last Appearance:** Date and time when the process was identified most recently.

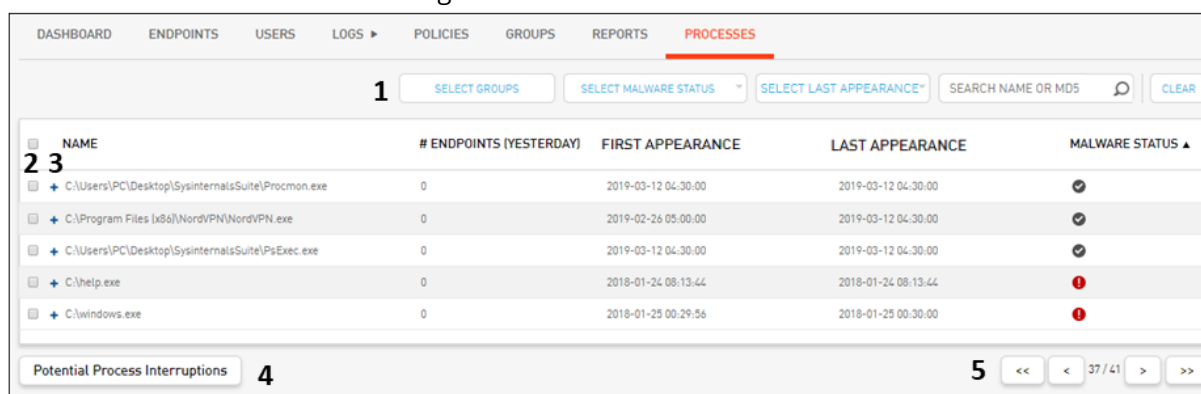
Malware Status: These icons indicate the potential security threat posed by the process, according to malware information available online:


-  : Classified as malware by VirusTotal.
- ◦  : Not classified as malware by VirusTotal.
-  : No information about the process is available in VirusTotal.

Click the icon and then click **Show Details** to view current information in VirusTotal.



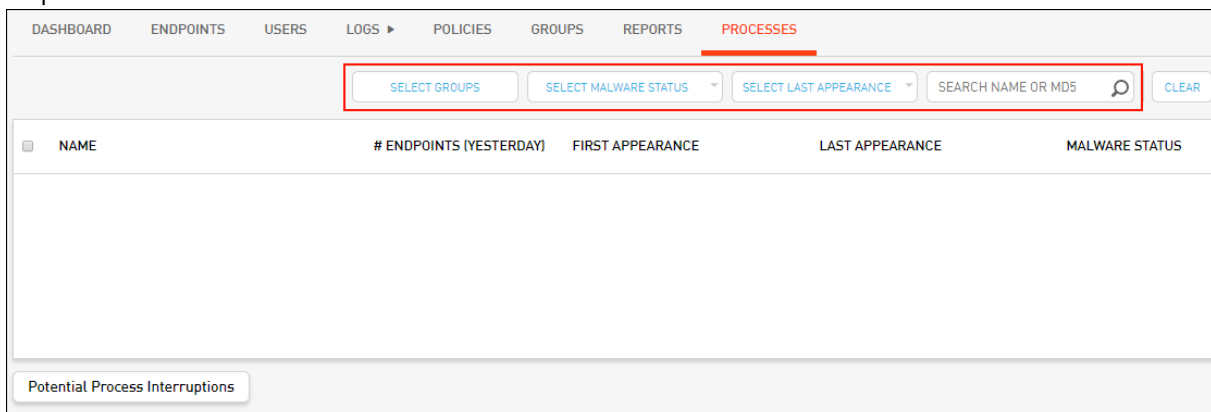
You can sort the grid according to any column. Additional features of the **Processes** tab are described in the table below the diagram.



Number	Feature	Description
1	Filtering options	Allow you to filter the Processes list according to various criteria. For details, refer to Filtering the Processes List .
2	Selection checkboxes	Allow you to select processes.
3	Expand icon	Clicking  displays additional details about the process. For more information, refer to Viewing Processes .
4	Potential Process Interruptions button	Clicking this button enables you to view logs for False Positive events that did not appear in the Dashboard because they were automatically solved by the Server. For details, refer to Viewing Processes .
5	Navigation bar	Enables you to quickly access other pages of the list.

Filtering the Detection and Response Monitoring Environment Processes List

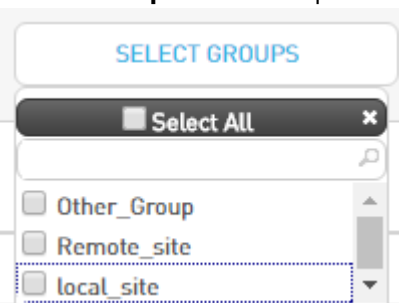
The filtering options above the Processes list enable you to search for processes according to a variety of criteria. The filtering options can be combined to define very specific search criteria, as required.



The screenshot shows the 'PROCESSES' tab in the top navigation bar. Below the navigation bar, a red box highlights the filtering section, which includes four buttons: 'SELECT GROUPS', 'SELECT MALWARE STATUS', 'SELECT LAST APPEARANCE', and a search input field labeled 'SEARCH NAME OR MD5' with a magnifying glass icon and a 'CLEAR' button. Below the filtering section is a table with the following headers: 'NAME', '# ENDPOINTS (YESTERDAY)', 'FIRST APPEARANCE', 'LAST APPEARANCE', and 'MALWARE STATUS'. The table body is currently empty. At the bottom of the interface, there is a button labeled 'Potential Process Interruptions'.

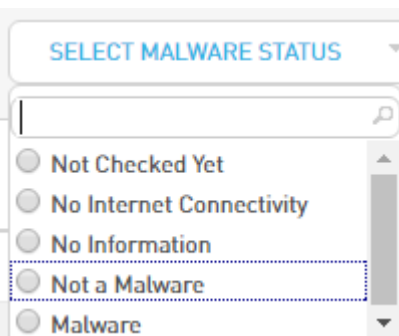
The filtering options are:

Select Groups: Filters for processes that ran in a selected endpoints Group.

- 

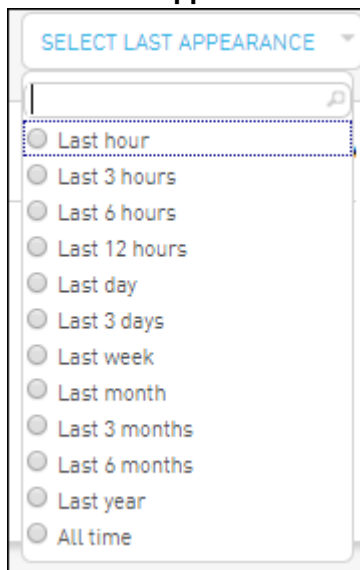
The screenshot shows the 'SELECT GROUPS' dropdown menu. It has a search bar at the top. Below the search bar, there is a list of groups: 'Other_Group', 'Remote_site', and 'local_site'. The 'local_site' group is selected, indicated by a blue dashed box around it.

Select Malware Status: Filters for processes that correspond to a specific malware status.

- 


The screenshot shows the 'SELECT MALWARE STATUS' dropdown menu. It has a search bar at the top. Below the search bar, there is a list of malware statuses: 'Not Checked Yet', 'No Internet Connectivity', 'No Information', 'Not a Malware', and 'Malware'. The 'Not a Malware' status is selected, indicated by a blue dashed box around it.

Select Last Appearance: Filters for processes that were identified during a selected timeframe.



- **Search Name Or MD5:** Supports a free text keyword search according to process name or MD5 identifier.

To filter the Processes list:

1. At the top of the **Processes** tab, select the relevant filters from each list, and/or enter the required term in the **Search Name Or MD5** field.
2. Click .
The Processes list is filtered according to the selected criteria.
3. To clear filtering, click **CLEAR**.

Analyzing Processes in the Detection and Response Management Console

Viewing Processes in the Detection and Response Management Console

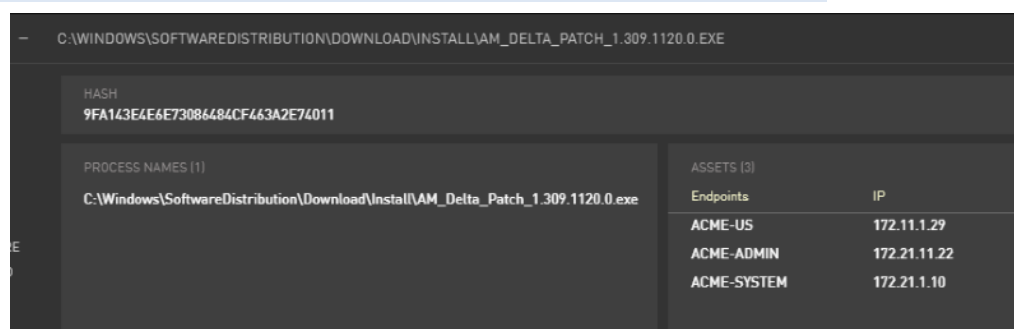
The **Application Control** menu of the Detection and Response Management Console lets you view and analyze processes that are running or have run on endpoints reporting to the Detection and Response Server. Any process that was monitored by the Detection and Response driver can be viewed on this page, regardless of whether or not the process involved suspicious events that were detected/prevented by the Agent.

The main features of the **Application Control** page are described in the table below the diagram.

The screenshot shows the 'APPLICATION CONTROL' interface. At the top, it says '1 of 429 Processes selected'. Below this is a filter bar with 'FILTER BY:' and dropdowns for 'STATUSES', 'REPUTATION', and 'LAST 3 MONTHS'. To the right of the filter bar is a search bar labeled '2' and a column configuration icon labeled '3'. The main area is a table with columns: NAME, STATUS, # ASSETS (YESTERDAY), FIRST APPEARANCE, LAST APPEARANCE, and REPUTATION. The table lists various system processes like 'C:\WINDOWS\SOFTWARE\...'. A process is selected with a checkmark, and a details panel on the left is expanded, labeled '4'. At the bottom, there are buttons for 'MANAGE PROCESS', 'BLOCK PROCESS', and 'EXPORT', with the 'MANAGE PROCESS' button labeled '6'. A large number '5' is placed over the table area.

Number	Feature	Description
1	Filtering tool	Allow you to filter the Processes list according to Blocked / Unblocked processes, process reputation and/or last appearance.
2	Search tool	Allow you to filter processes according to keyword search. The Processes list is filtered as you type.
3	Configure Columns tool	Allows you to control which columns of the grid are displayed.
4	Expand/Collapse icons	Click to show/hide more details about the process and the endpoints affected by them.

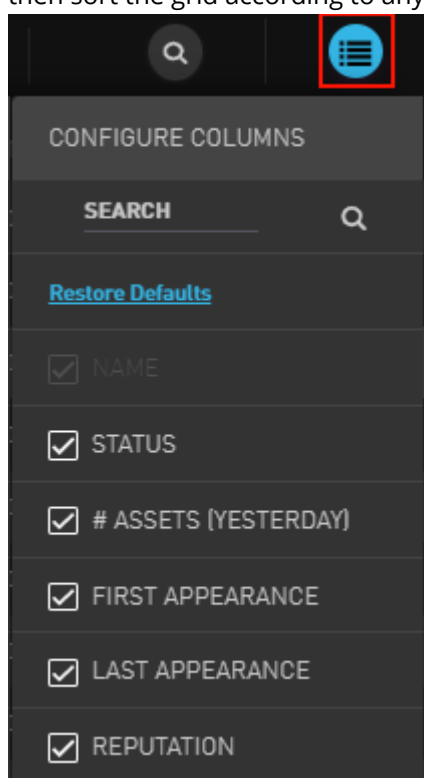
Number	Feature	Description
--------	---------	-------------






- | | | |
|---|--------------------------------------|--|
| 5 | Processes grid | Lists general information about each process. For details, refer to Understanding the Detection and Response Management Console Processes Grid (below). |
| 6 | Manage Process
actions bar | Allows you to perform administrative operations on one or more processes. For more information, refer to Managing Processes in the Detection and Response Management Console . |

Understanding the Detection and Response Management Console Processes Grid

The information provided in the grid is described in the table below. You can control the column display by clicking the Configure Columns icon and selecting the columns you want to see. You can then sort the grid according to any column.



Column	Description / Notes
Name	Full path of the process.
Status	EPR status of the process (Blocked or Unblocked). For more information, refer to Managing Processes in the Detection and Response Management Console .
# Assets (Yesterday)	Number of Assets on which the process was identified during the most recent midnight to midnight 24-hour period. For example, if you are looking at the list on Wednesday at 10 am, the value reflects the number of Assets affected between midnight Tuesday and midnight Wednesday.
First Appearance / Last Appearance	Date when the process was first identified / Date when the process was most recently seen.
Reputation	<p>Potential security threat posed by the process, according to malware information available online:</p> <ul style="list-style-type: none"> : Classified as malware by VirusTotal. : Not classified as malware by VirusTotal, but considered by Detection and Response to be potentially malicious nonetheless. : No information about the process is available in VirusTotal.

Managing Processes in the Detection and Response Management Console

When you select one or more processes in the **Application Control** menu of the Detection and Response Management Console (by checking their boxes), the **Manage Process** actions bar appears at the lower left corner of the page.

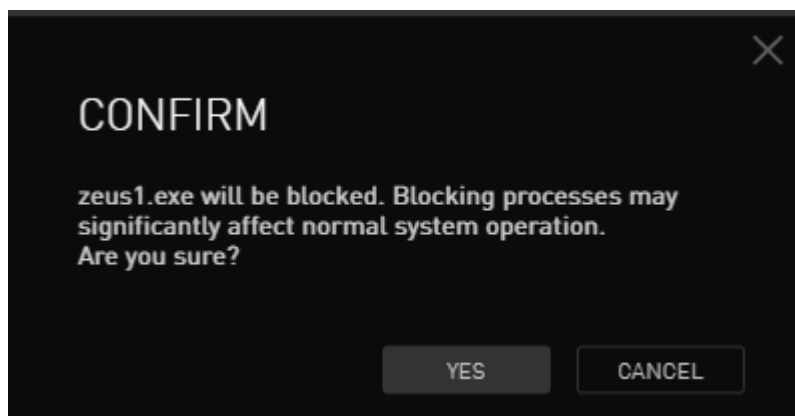


Block Process

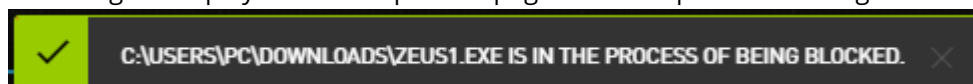
Blocking a process is an Endpoint Protection and Response (EPR) mechanism that has the following effects:

- All currently running instances of the selected process (on any Asset) are killed.
- All future attempts to execute the selected process (on any Asset) are blocked.

To block selected processes, select **Block Process** and click **Yes** in the confirmation popup.



A message is displayed at the top of the page while the process is being blocked.

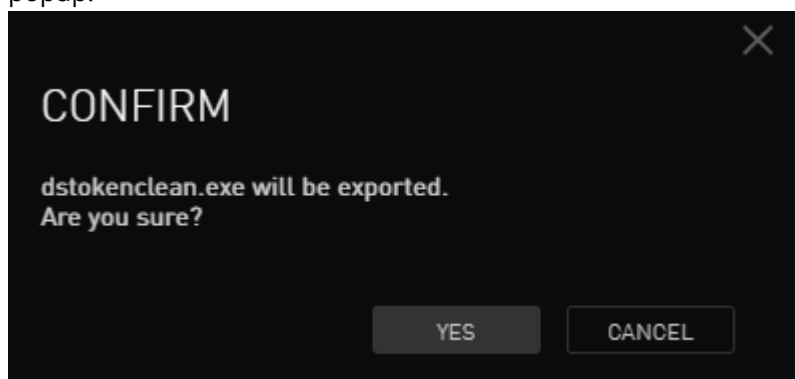


To lift the block, select the process and click **Unblock Process**.

Export

This action enables you to export selected processes to an Excel worksheet.

To export the processes that you have selected, select **Export** and click **Yes** in the confirmation popup.



Viewing and Managing Exceptions in the Detection and Response Monitoring Environment

Policies Overview

A policy, also known as an Exception, is a rule created by Detection and Response Monitoring Environment administrators that instructs Detection and Response to permit an action that would normally be blocked by Detection and Response. Detection and Response allows you to create an unlimited number of Exceptions.

As you add more policies, the policies can be prioritized in order of precedence. This gives you control over which policies will be enforced in the event that different policies contradict one another. (Once a match is found, the process stops.) In addition, you can temporarily disable any policy, as required.

To help you manage your set of policies efficiently, the Policies list in the Detection and Response Monitoring Environment includes information about which Groups (if any) a policy is assigned to, and the frequency with which a policy had matches. Policies that are not in use can be disabled.

The following sections describe how to work with policies:

- [Understanding the Policies Tab](#): Presents an overview of the **Policies** tab.
- [Adding Policies](#): Describes how to create a new policy and details the main components of a policy.
- [Managing Policies](#): Explains administrative actions (e.g., updating, disabling, etc.) that may be performed on policies.
- [Creating and Maintaining the Default Policy Set](#): Explains how to build and manage a collection of Exceptions that apply to all endpoints.
- [Applying Policies to Endpoint Groups](#): Explains how to assign policies to different Groups.

Understanding the Policies Tab

The **Policies** tab allows you to view, add and manage policies. The Search tool at the upper right corner lets you filter the Policies list according to a keyword (all or part of a policy's name, command line or Protection Module). The buttons at the lower left corner enable you to perform various [administrative operations](#), such as adding, importing/exporting and disabling policies.

DASHBOARD	ENDPOINTS	USERS	LOGS ▶	POLICIES	GROUPS	REPORTS	PROCESSES
-----------	-----------	-------	--------	-----------------	--------	---------	-----------

3 policies

NAME	PROTECTION MODULE	INITIATOR	SIGNED BY	TARGET	LAST MODIFIED ▼	ASSIGNMENT	MATCHES	STATUS
MDS_E0_240619_powershel	Unauthorized Access Request	C:\WINDOWS\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Microsoft Windows	C:\WINDOWS\system32\lsass.exe	2019-06-26 10:01:34	Assigned	0	Enabled
MDS_E0_290619_powershell_dnein...	Evasion	*[windows\Sys*]\WindowsPowerShell\v1.0\powershell.exe	Microsoft Windows*	*[windows\sys*]\netsh.exe	2019-06-29 15:51:05	Assigned	4	Enabled
MDS_T0_300918_POWERSHELL_DE...	Shell Activity	*[WindowsPowerShell]\powershell.exe	Microsoft Windows	*[DismHost.exe	2018-12-13 16:31:02	Assigned	37	Enabled

The grid in the center of the page lists the following information about each policy:

Column	Description
Name	A user-defined name that identifies the policy.
Protection Module	Type of defense provided.
Initiator	The path / name of the process performing the event defined in the policy.
Signed By	The organization / company that digitally signed the process.
Target	The path/name of the entity impacted by the policy. A target can range from one specific file to all entities on an endpoint (indicated by *).
Last Modified	Date and time of the most recent update to the policy.
Assignment	Indicates whether the policy is currently assigned to any Groups.
Matches	A counter showing the number of endpoints on which the policy had matches. When hovering over the counter, timestamps of first and last match dates, a list of affected endpoints, and the Agent/BPM versions of the endpoints are displayed.

Column

Description

Policy Matches

MDS_VB_151019_VpxClient_E

First Match: 2019-10-15 15:00:00

Last Match: 2019-11-18 11:00:00

Affected Endpoints: 26

ID	Name	Last Match
185	NYO-ADMINTERM	2019-11-18 11:00:00
127	DESKTOP-DF413D6	2019-11-18 11:00:00
61	OREN-PC	2019-11-17 19:00:00
225	aarazi-wks	2019-11-17 17:00:00
104	MICHAEL-PC	2019-11-17 17:00:00
30	IDAN-PC	2019-11-17 14:00:00
235	egordon-ltop	2019-11-17 14:00:00
24	AMICHA-PC	2019-11-17 13:00:00
97	ELIOR-LT	2019-11-17 13:00:00
179	GEORGE-PC	2019-11-17 12:00:00

Agent Version	BPM Version	Endpoints
2.18.16909.0	2.18.1188.0	12
2.18.17632.0	2.18.1215.0	10
2.18.17605.0	2.18.1198.0	8
2.18.17673.0	2.18.1218.0	7
2.18.17416.0	2.18.1161.0	7
Other Agent & BPM Versions		-

MATCHES ▼ STATUS

26 Enabled

18 Enabled

16 Enabled

16 Enabled

15 Enabled

14 Enabled

For more information about matching, refer to [Managing Policies](#).

Status **Enabled** or **Disabled**. Disabled policies are inactivated and not implemented.

Adding a Policy from the Policies Tab

Creating a new policy (Exception) consists of providing a name for the policy and specifying details about the process involved. In addition, you may include the new policy in the [Default Policy Set](#), or [assign it to one or more specific Groups](#).

Important

It is best practice to create policies from the Dashboard view, where you can start with a specific event and view prepopulated parameters for the Exception. For details, refer to [Adding an Exception from the Detection and Response Monitoring Environment Dashboard](#).

To add a new policy:

1. At the lower left corner of the **Policies** tab, click **Add policy**.
The **Add Policy** dialog opens.

The 'Add Policy' dialog box is shown with the 'Policy Details' tab selected. It contains the following fields:

- Name: [Text Input]
- Description: [Text Input]
- Protection Module: [Dropdown Menu]
- Initiator Path: [Dropdown Menu (Is)] [Text Input]
- Initiator Name: [Dropdown Menu (Is)] [Text Input]
- Initiator Publisher: [Text Input]
- Initiator MD5: [Text Input]
- Initiator Command Line: [Text Input]
- Parent Path: [Dropdown Menu (Is)] [Text Input]
- Parent Name: [Dropdown Menu (Is)] [Text Input]
- Parent Publisher: [Text Input]
- Parent MD5: [Text Input]
- Target Path: [Dropdown Menu (Is)] [Text Input]
- Target Name: [Dropdown Menu (Is)] [Text Input]

At the bottom of the dialog, there is a button labeled 'Assign Policy' and a 'Save' button. A 'Close' button is located at the bottom right of the dialog.

2. In the **Name** field, enter a logical name for the new policy.
3. If desired, in the **Description** field, enter notes or comments about the new policy.
4. From the **Protection Module** dropdown list, select the relevant Protection Module.
5. Specify initiator, parent and target parameters. For more information, refer to [Understanding the Policies Tab](#).

All parameters you define for the policy operate according to *AND* logic.

If you wish, define assignments for the policy by opening the **Assign Policy** frame. (If you don't want to assign the policy at this time, skip to Step 9.)

The 'Add Policy' dialog box is shown with the 'Assign Policy' tab selected. It contains the following options:

- ☐ Assign as a default policy
Default policies are shared with all client's PARANOID Servers which are connected to the Controller Server
- ☐ Assign to one or more groups
- ☒ Assign to none

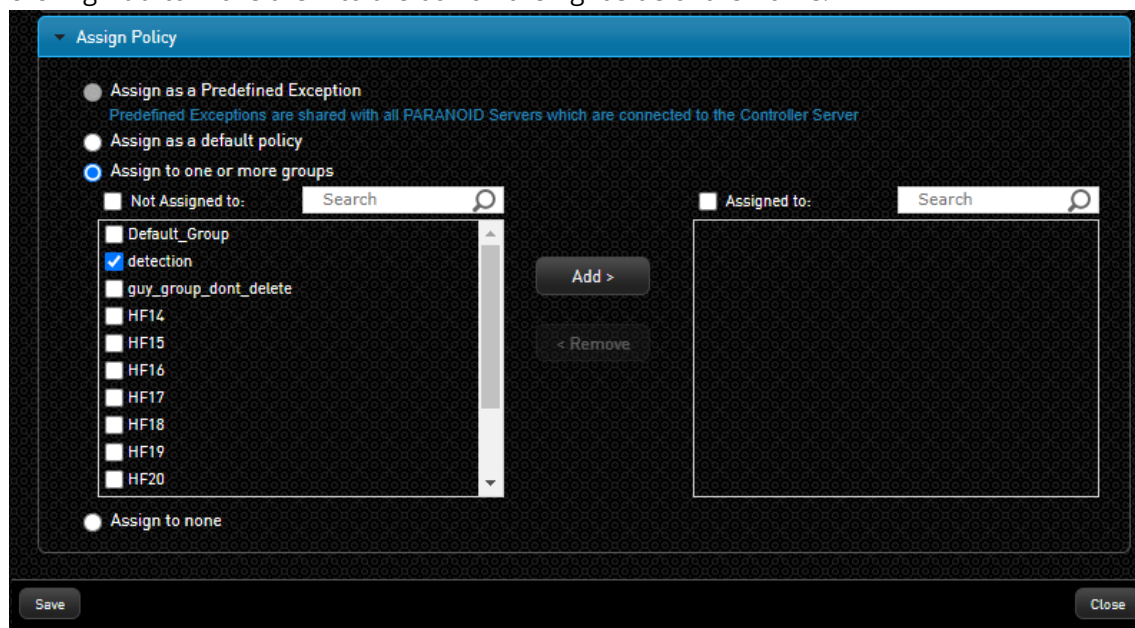
At the bottom of the dialog, there is a 'Save' button and a 'Close' button.

6.

7. Assign the policy in one of the following ways:

- **Assign as a default policy:** Select this radio button to add the new policy to the [Default Policy Set](#). Default policies are applied to all endpoints connected to the Detection and Response Server. In multi-server setups where servers are connected to the Controller Server, these policies are also automatically distributed to the other Detection and Response Servers in the environment as default policies.

Assign to one or more groups: Select this radio button to apply the policy to specific Groups. Build your **Assigned to** list by selecting Groups from the box on the left side of the frame, and clicking **Add** to move them to the box on the right side of the frame.



8. Click **Save**.

The policy is saved, and a confirmation message is displayed at the top of the dialog.

9. To add another policy, repeat Steps 2-8.

10. When you are finished creating policies, exit the **Add Policy** dialog by clicking **Close**.

Managing Policies in the Detection and Response Monitoring Environment

The following sections describe how to perform various administrative actions on one or more policies. The available options are:

- [Exporting and Importing Policies](#)
- [Disabling and Enabling Policies](#)
- [Updating Policies](#)
- [Managing Matching Activities](#)
- [Deleting Policies](#)

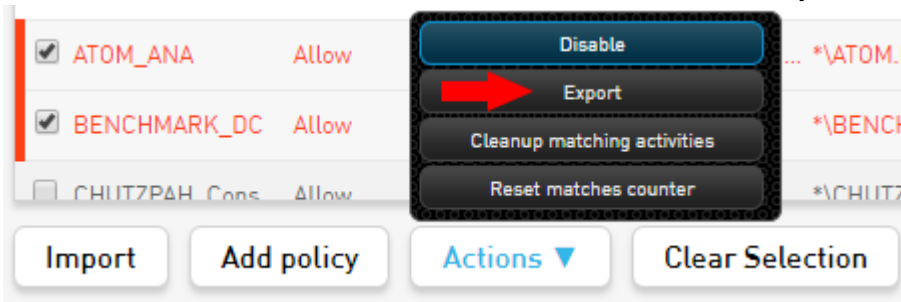
Exporting and Importing Policies

Detection and Response supports the export and import of policies for backup purposes, or for deployment of a defined group of policies on other Detection and Response servers. Policies are exported as an XML file.

To export policies:

1. On the left side of the **Policies** grid, select the checkboxes of the policies that you want to export. Selecting the checkbox in the **Name** column header selects all the checkboxes.

At the bottom of the **Policies** tab, click **Actions** and then select **Export**.

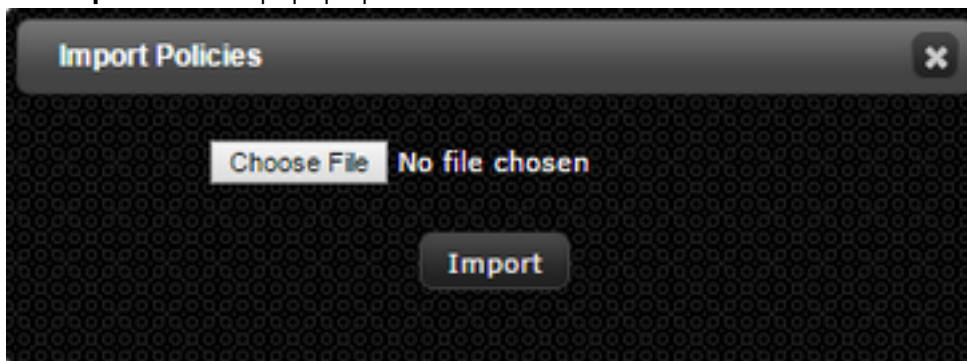


2. The selected policies are downloaded as an XML file.

To import policies:

At the lower left corner of the **Policies** tab, click **Import**.

The **Import Policies** popup opens.

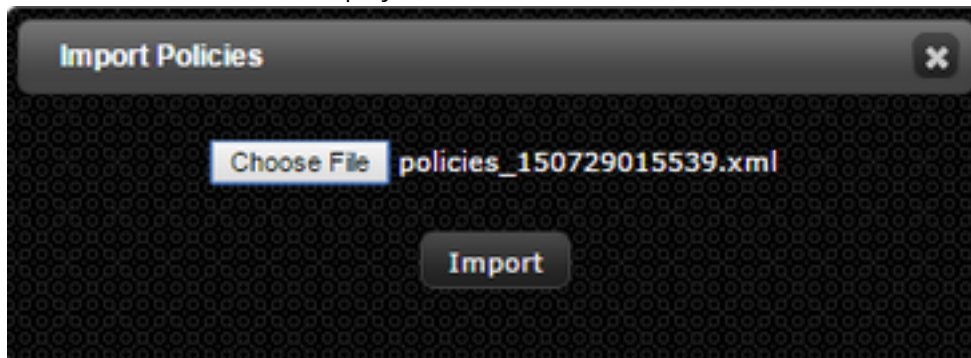


- 1.
2. Click **Choose File**.

The **Open** dialog appears.

Navigate to the required .xml file, and click **Open**.

The selected file name is displayed next to the **Choose File** button.



3.

4. Click **Import**.

The policies are imported and listed in the Policies grid.

Disabling and Enabling Policies

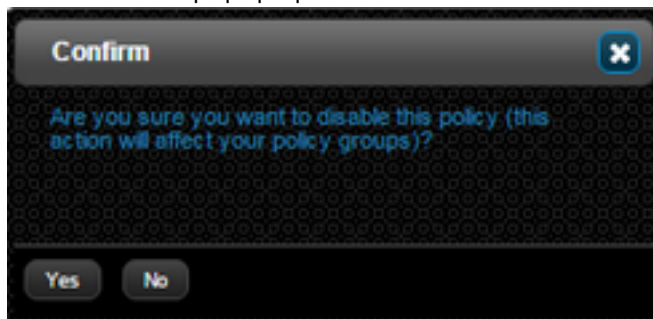
The Disable feature inactivates a selected policy. Use this option when you need to suspend one or more policies temporarily.

To disable and enable a policy:

1. On the left side of the **Policies** grid, select the checkbox of the policy that you want to disable.

At the bottom of the page, click **Actions** and then select **Disable**.

A confirmation popup opens.



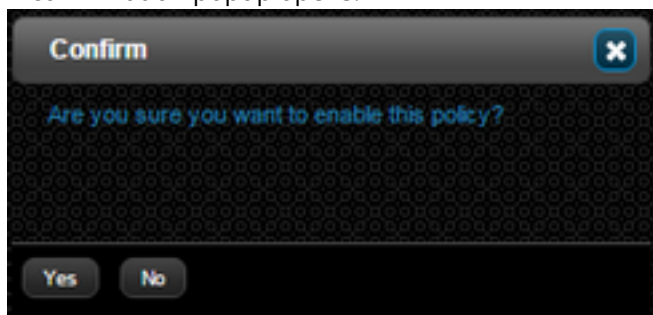
2.

3. Click **Yes**.

The policy is inactivated.

To reactivate the policy, select the checkbox of the policy. Click **Actions** and then select **Enable**.

A confirmation popup opens.



4.

5. Click **Yes**.

The policy is re-activated.

Updating Policies

The Edit Policy feature allows you to update any parameter of an existing policy, including adding or changing assignments to Groups.

To update a policy:

From the Policies grid, select the row of the policy that you want to update.

The **Edit Policy** dialog opens, with read-only parameters.

Edit Policy

Policy Details

Name: FPC_SG_301017_Explorer_DC

Description:

Protection Module: Data Corruption

Initiator Path: Is C:\WINDOWS\

Initiator Name: Is Explorer.EXE

Initiator Publisher: Microsoft Windows

Initiator MD5: F2E16463663A8DFA8638A6C1B4125129

Parent Path: Is C:\WINDOWS\system32\

Parent Name: Is userinit.exe

Parent Publisher: Microsoft Windows

Parent MD5: 517FE50B55C9D46844E4D93952DA7CE4

Target Path: Is \REGISTRY\USER\S-1-5-21-831613323-794070214-3480653525-100

Target Name: Is Generation

Assign Policy

Edit **Close**

- 1.
2. At the bottom of the dialog, click **Edit**.
The parameters become editable.
3. Update the parameters in the **Policy Details** and the **Assign Policy** frames, as required.
For more information about the parameters and options, refer to [Adding Policies](#).
4. Click **Save**.
The dialog closes, and your changes are saved in the system.

Managing Matching Activities

The **Matches** column of the Policies grid is a counter showing the number of endpoints on which the policy had matches. When hovering over the counter, timestamps of first and last match dates, as well as Agent/BPM versions of the endpoints are displayed.

NAME	TYPE	PROTECTION MODULE	INITIATOR	SIGNED BY	MD5	TARGET	ASSIGNMENT	MATCHES	STATUS
AAAAa	Allow	*	*	*	*	*	Unassigned	0	Enabl
ATOM_ANA	Allow	ABNORMAL_NETWORK_AC...	*ATOM.EXE	GitHub, Inc.	*	*.443	Unassigned	0	Enabl
<input checked="" type="checkbox"/> BENCHMARK_DC	Allow	DATA_CORRUPTION	*BENCHMARK3.EXE	*	2F90DAF2EBCC5BB661D3D804881...	*%o.txt	Unassigned	0	Enabl

Import Add policy Actions ▼ Clear Selection

Policy Matches

MDS_VB_151019_VpxClient_E

First Match: 2019-10-15 15:00:00
Last Match: 2019-11-18 11:00:00
Affected Endpoints: 26

ID	Name	Last Match
185	NYO-ADMINTERM	2019-11-18 11:00:00
127	DESKTOP-DF413D6	2019-11-18 11:00:00
61	OREN-PC	2019-11-17 19:00:00
225	aarazi-wks	2019-11-17 17:00:00
104	MICHAEL-PC	2019-11-17 17:00:00
30	IDAN-PC	2019-11-17 14:00:00
235	egordon-ltop	2019-11-17 14:00:00
24	AMICHAH-PC	2019-11-17 13:00:00
97	ELIOR-LT	2019-11-17 13:00:00
179	GEORGEPC-PC	2019-11-17 12:00:00

Agent Version	BPM Version	Endpoints
2.18.16909.0	2.18.1188.0	12
2.18.17632.0	2.18.1215.0	10
2.18.17605.0	2.18.1198.0	8
2.18.17673.0	2.18.1218.0	7
2.18.17416.0	2.18.1161.0	7
Other Agent & BPM Versions		-

You can perform the following actions to manage matching activities:

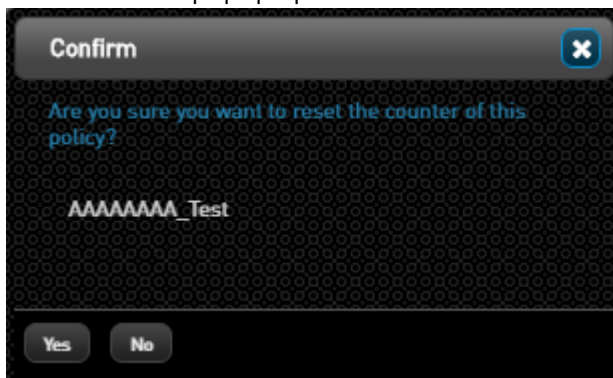
- Reset the Matches counter
- Cleanup matching activities

Resetting the Matches Counter

This action resets the count in the **Matches** column to zero.

To reset the Matches counter of a policy:

1. At the left side of the Policies grid, select the checkbox of the relevant policy.
At the bottom of the page, click **Actions** and then select **Reset matches counter**.
A confirmation popup opens.



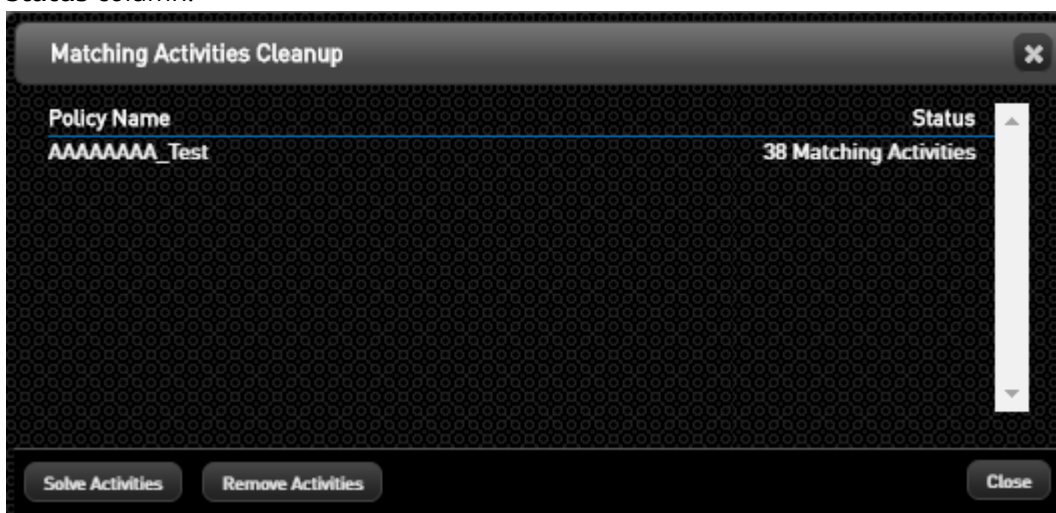
- 2.
3. Click **Yes**.
The counter is reset to zero.

Cleaning Up Matching Activities

This action clears matching activities from the Dashboard by solving or removing them.

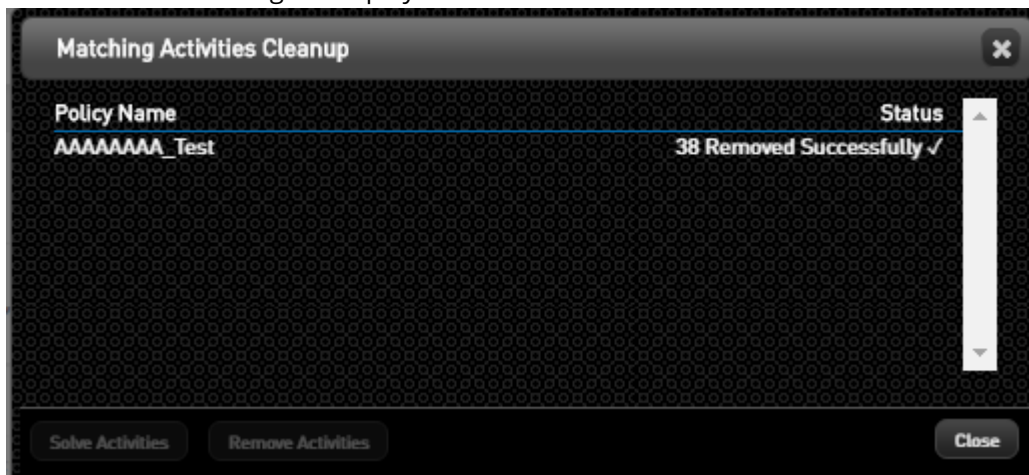
To clean up matching activities:

1. At the left side of the Policies grid, select the checkbox of the relevant policy.
At the bottom of the page, click **Actions**, and then select **Cleanup matching activities**.
The **Matching Activities Cleanup** dialog opens, listing the number of matching activities in the **Status** column.



- 2.
3. In the lower left corner of the dialog, click **Solve Activities** or **Remove Activities**. (For more information about these actions, refer to [Handling Events in the Dashboard View](#).)

A confirmation message is displayed in the **Status** column.



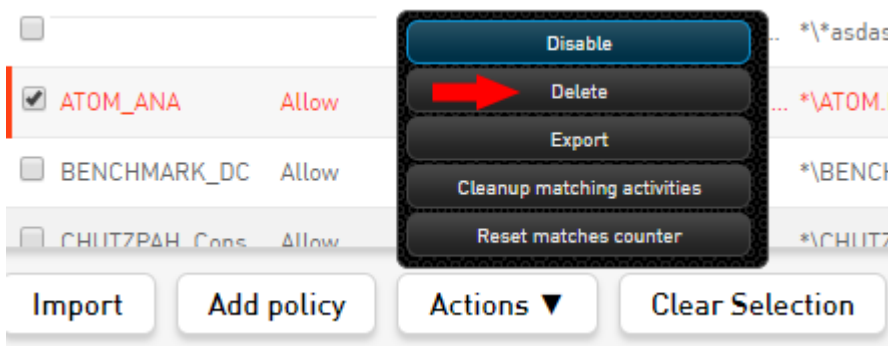
4. To exit the dialog, click **Close**.

Deleting Policies

Deleting a policy permanently removes the policy from the system. You can delete unnecessary policies by using the Delete action at the bottom of the Policies grid.

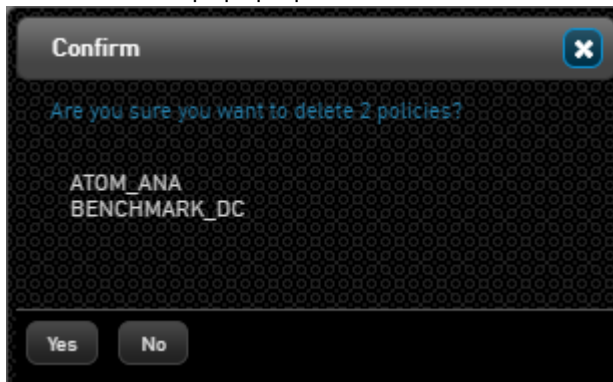
To delete policies:

1. At the left side of the Policies grid, select the checkboxes of the policies that you want to remove. At the bottom of the page, click **Actions** and select **Delete**.



- 2.

A confirmation popup opens.



3. Click **Yes**.

The selected policies are removed from the Policies grid, and are deleted from the system.

Creating and Maintaining the Default Policy Set

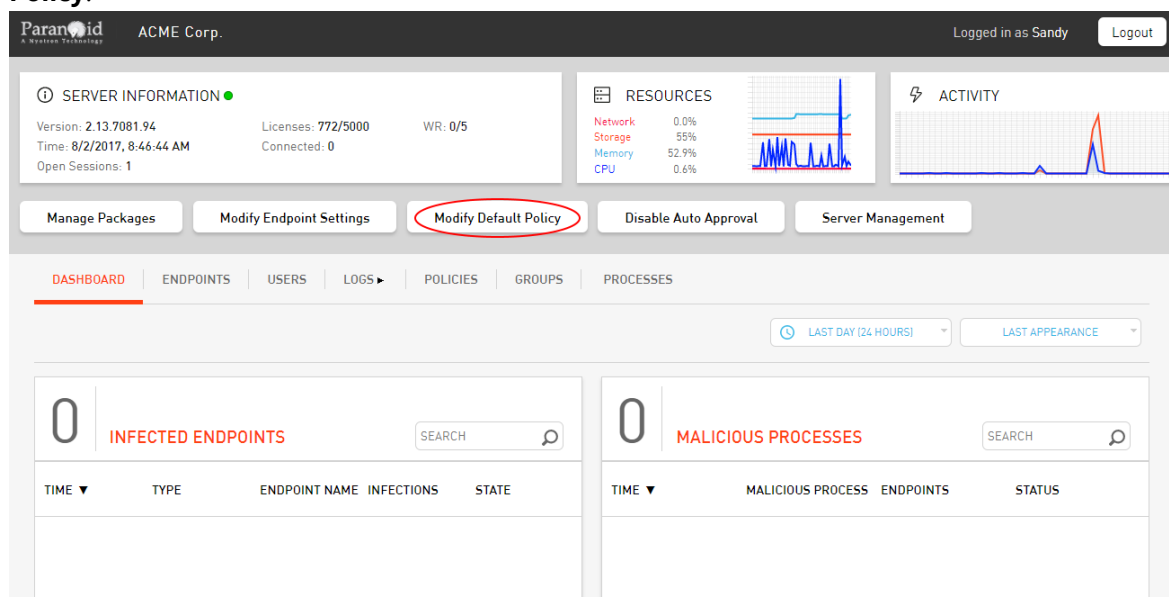
The Default Policy Set is a collection of policies (Exceptions) that apply to all server endpoints. In multi-server setups where servers are connected to the Controller Server, these policies are automatically shared with all Detection and Response Servers in the customer environment.

After assigning policies to the Default Policy Set, you can specify policy enforcement settings by defining order of priority. For more information, refer to [Maintaining the Default Policy Set](#).

Since the Default Policy Set impacts all Groups, it is recommended that it include only Exceptions that are relevant to all endpoints. Policies that affect only a portion of end users (e.g., developers, managers, etc.) should not be part of the Default Policy Set, but should be assigned to the relevant Groups. For more information, refer to [Applying Policies to Endpoint Groups](#).

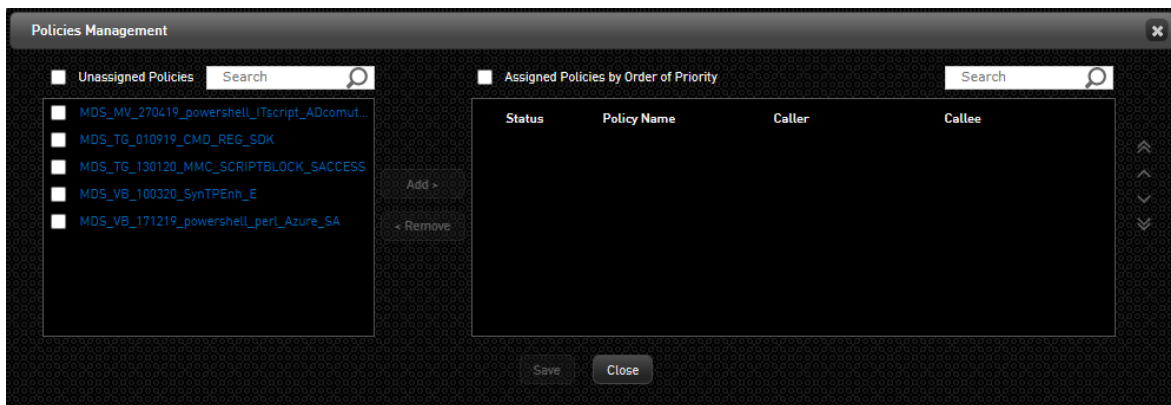
To build the Default Policy Set:

At the top of the Detection and Response Monitoring Environment console, click **Modify Default Policy**.

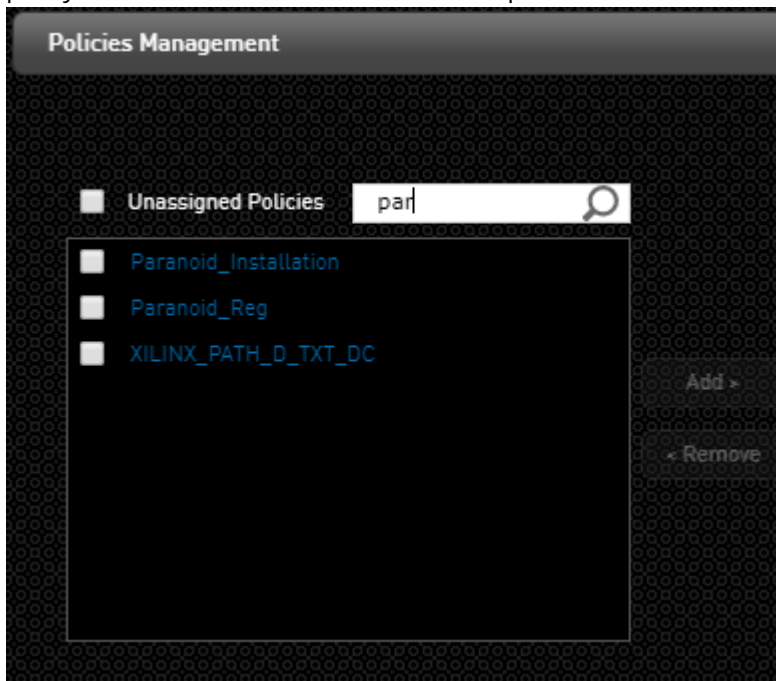


- 1.

The **Policies Management** dialog opens. By default, the Default Policy Set is empty, and all defined policies are listed on the left side, under **Unassigned Policies**.

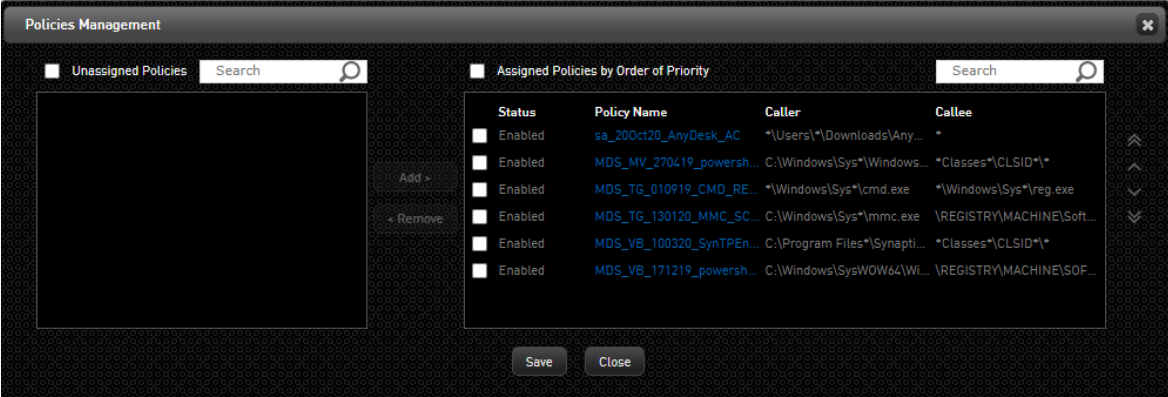


From the **Unassigned Policies** list, select the checkboxes of the policies that you want to add to the Default Policy Set. (To select all the policies, select the checkbox at the top, next to **Unassigned Policies**.) To filter the list so you can easily find a policy, enter all or part of the policy name in the **Search** field. For example:



- 2.
3. After selecting the policies to add, click **Add**.

The selected policies, together with basic policy parameters, are transferred to the list of policies that appears on the right side of the dialog. These are the policies that are assigned to the Default Policy Set.



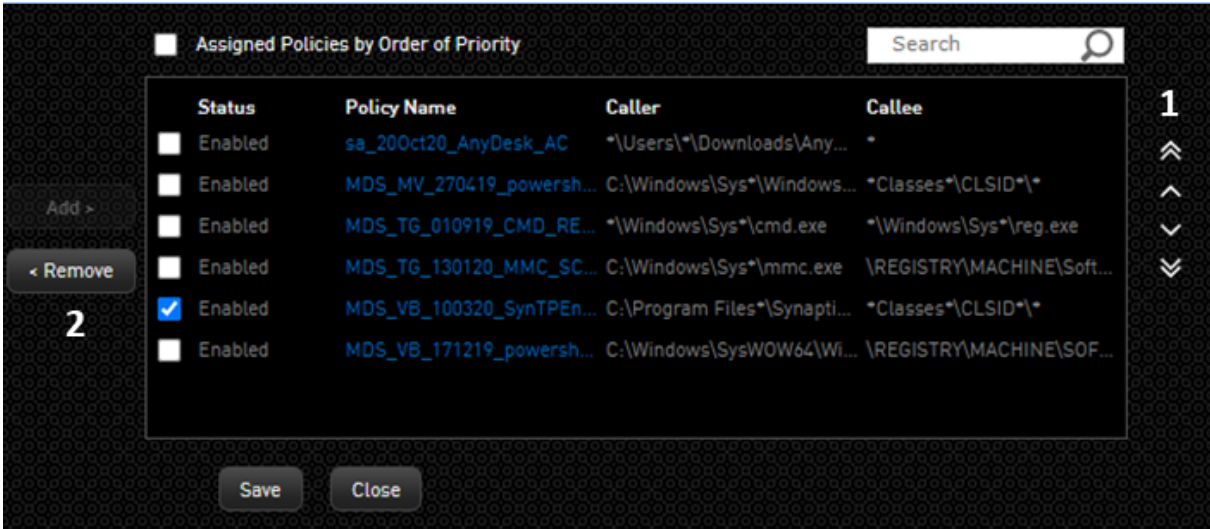
- 4. If desired, you may configure policy enforcement settings at this time (e.g., which policies take precedence over other policies). For details, refer to Maintaining the Default Policy Set (below).
- 5. Click **Save**.
A confirmation message is displayed at the top of the popup, and the default policy set is saved.

Maintaining the Default Policy Set



The **Policies Management** dialog provides several features that enable you to control how the exceptions in the Default Policy Set are enforced. The options are described in the table below the diagram.

Note

If a policy is assigned to both the Default Policy Set and to one or more specific Groups, the Group policy enforcement settings determine how the policy is applied.



Number	Feature	Description
1	Priority management	This feature lets you control which policies will be enforced in the event that policies in the Default Policy Set contradict one another. Select a single

Number	Feature	Description
	arrows	policy by checking its checkbox, and then use the arrows to move it into the position of precedence in the list. The policy that is listed first is carried out first, and so on. Clicking  or  moves a policy to the beginning or the end of the list.
2	Remove button	This feature allows you to remove policies from the Default Policy Set. Select the relevant policies, and then click Remove . The selected policies are transferred to the left side of the Policies Management dialog.

Applying Policies to Endpoint Groups

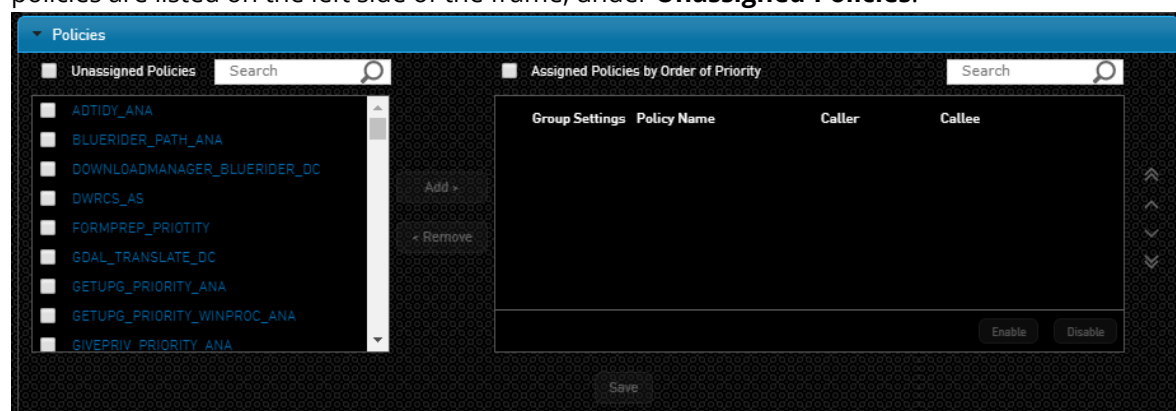
Policies do not have any impact on event handling unless they are applied to one or more Groups. The procedure below explains how to assign policies to a Group. After assigning policies to the Group, you can specify policy enforcement settings by defining order of priority.

To assign policies to a Group:

1. From the **Groups** tab, click in the row of the relevant Group.

The **Endpoints Group** dialog opens.

Open the **Policies** frame. By default, no policies are assigned to the Group, and all defined policies are listed on the left side of the frame, under **Unassigned Policies**.



- 2.
3. From the **Unassigned Policies** list, select the checkboxes of the policies that you want to apply to the Group. (To select all the policies, select the checkbox at the top, next to **Unassigned Policies**.) To filter the list so you can easily find a policy, enter all or part of the policy name in the **Search** field.
4. After selecting the policies to add, click **Add**.
The selected policies, together with basic policy parameters, are transferred to the list of policies that appears on the right side of the frame. These are the policies that are assigned to the Group.
5. To save your changes, click **Save**.

Maintaining Group Policies

The **Policies** frame of the **Endpoints Group** dialog provides several features that enable you to define enforcement settings for the policies assigned to the Group, including:

- Organizing policies according to priority
- Removing policies from the Assigned Policies list



For more details about how to use these features, refer to [Creating and Maintaining the Default Policy Set](#).


Configuring Automatic Exception Retirement

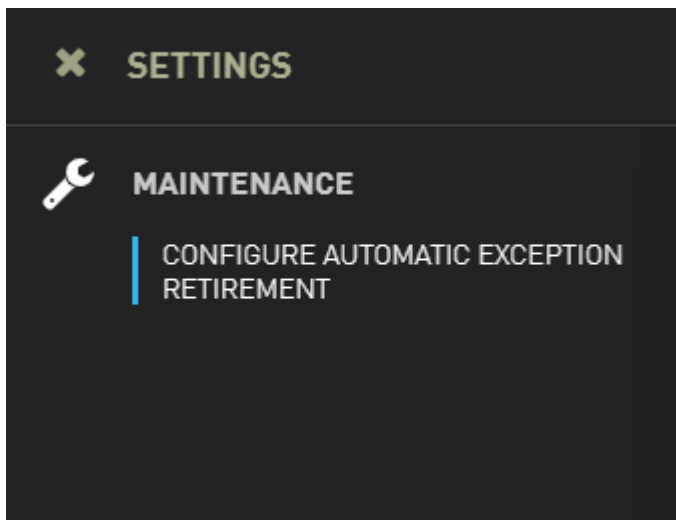
Automatic Exception Retirement (AER) is a mechanism that automatically removing inactive Exceptions from the system. AER reduces bandwidth, reduces potential security breaches, and helps keep your set of Exceptions manageable.

Inactive Exceptions are defined as those that have not have a match AND whose settings have not been updated within a specified period of time. The time period that defines inactivity is configured by the user when specifying AER settings. Supported time frames range from 30 to 550 days.

By default, AER is disabled. The following procedure explains how to enable and configure AER from the Detection and Response Management Console.

To enable and configure AER:

1. In the upper right corner of the Detection and Response Management Console, click  to open the **Settings** menu. Then select **Configure Automatic Exception Retirement**.



The **Configure Automatic Exception Retirement** pane is displayed.

Click **Enabled** to make the settings editable. Then, in the field below, enter the number of days after which inactive Exceptions will be automatically deleted. The default value is 90 days.

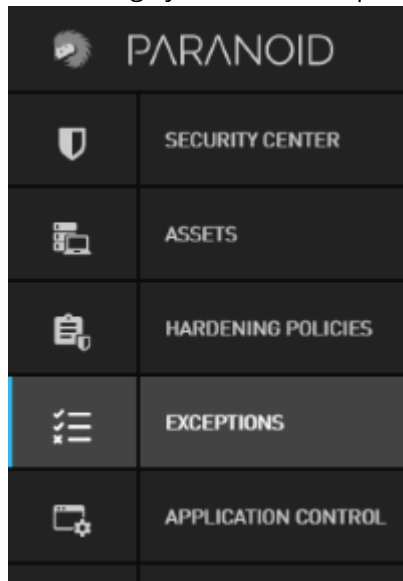


- 2.
3. To save your changes, click **Apply**.

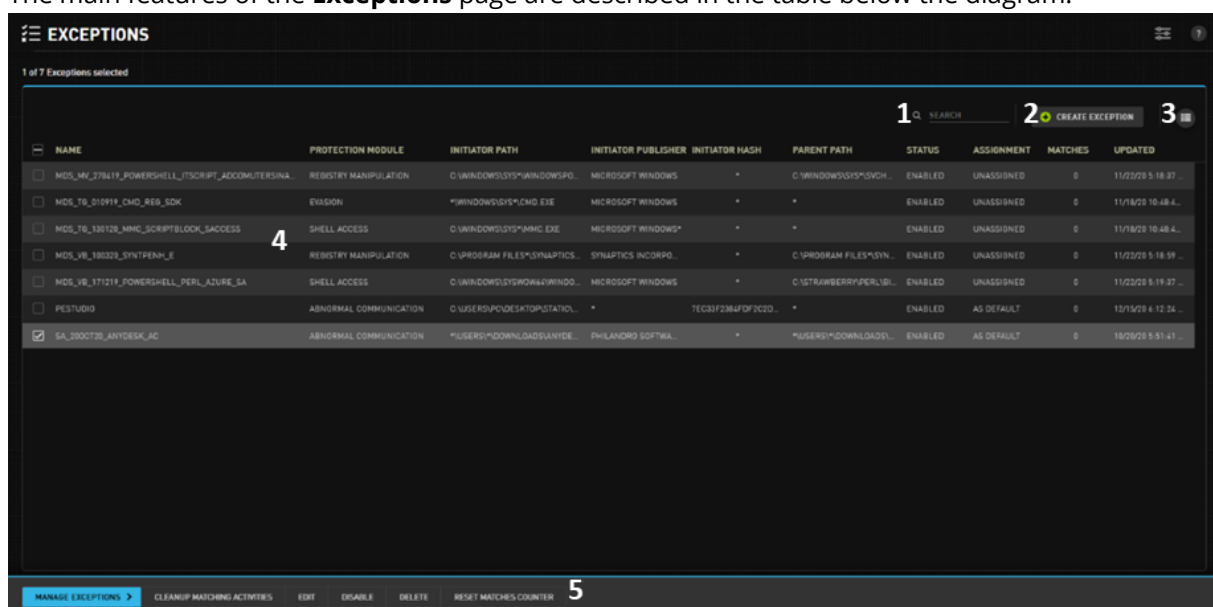
Viewing and Managing Exceptions in the Detection and Response Management Console

Working with the Exceptions Menu

The **Exceptions** menu of the Detection and Response Management Console lets you view, update and manage your set of Exceptions.



The main features of the **Exceptions** page are described in the table below the diagram.



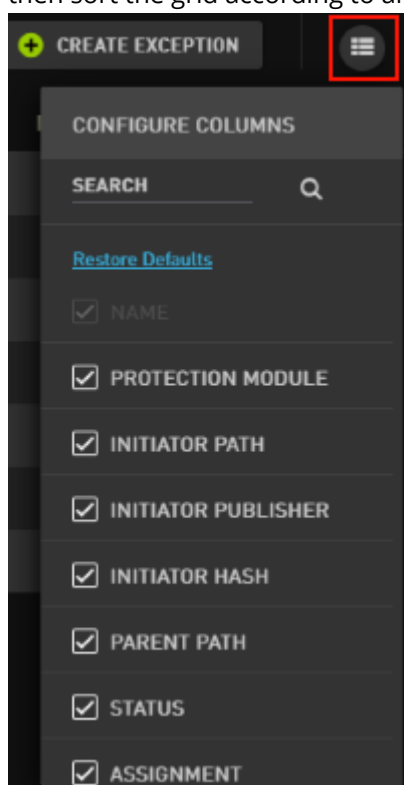
Number	Feature	Description
--------	---------	-------------

- | | | |
|---|-------------|--|
| 1 | Search tool | Allow you to filter Exceptions according to keyword search. The Exceptions list is filtered as you type. |
|---|-------------|--|

Number	Feature	Description
2	Create Exception button	Enables you to add a new Exception. For details, refer to Adding Exceptions .
3	Configure Columns tool	Allows you to control which columns of the grid are displayed.
4	Exceptions grid	Lists general information about each Exception. For details, refer to Understanding the Exceptions Grid (below).
5	Manage Exceptions actions bar	Allows you to perform administrative operations on one or more Exceptions. For more information, refer to Exception Management .

Understanding the Exceptions Grid

The information provided in the grid is described in the table below. You can control the column display by clicking the Configure Columns icon and selecting the columns you want to see. You can then sort the grid according to any column.



Column	Description / Notes
Name	A user-defined name that identifies the Exception.
Protection Module	Type of defense provided.

Column	Description / Notes
Initiator Path	The path of the process performing the event defined in the Exception.
Initiator Publisher	The organization / company that digitally signed the process.
Initiator Hash	The MD5 identifier of the process.
Parent Path	The path of the process that created the Initiator process.
Status	Enabled or Disabled . Disabled Exceptions are inactivated and not implemented.
Assignment	Indicates whether the Exception is currently assigned. If the Exception is assigned to specific Groups, the number of affected Groups is displayed.
Matches	A counter showing the number of endpoints on which the Exception had matches.
Updated	Date and time of the most recent update to the Exception.

Adding Exceptions in the Detection and Response Management Console

Creating a new Exception consists of providing a name for the Exception and specifying details about the Initiator and Target of the process involved. In addition, you may include the new Exception in the [Default Policy Set](#), or assign it to one or more Groups.

Important

It is best practice to create Exceptions from the Drill Down view of the Security Center, where you can start with a specific event and view prepopulated parameters for the Exception.

To add a new Exception:

At the upper right corner of the **Exceptions** page, click **Create Exception**.



The **New Exception** page opens.

X NEW EXCEPTION

NAME *

DESCRIPTION

PROTECTION MODULE

ABNORMAL COMMUNICATION

INITIATOR

PROCESS

PATH

NAME

IS

PUBLISHER

IS

HASH

COMMAND LINE

PARENT

PATH

NAME

IS

PUBLISHER

IS

HASH

TARGET

IP

IS

PORT

IS

ASSIGN EXCEPTION

☐ ASSIGN AS A DEFAULT POLICY

☐ ASSIGN TO ONE OR MORE GROUPS

☒ ASSIGN TO NONE

SAVE

CANCEL

2. In the **Name** field, enter a logical name for the Exception. It is recommended (but not required) to enter notes or comments about the new Exception in the **Description** field.
3. Select the appropriate Protection Module from the **Protection Module** dropdown list.
4. Specify parameters for the Initiator and Parent. When defining paths and command line, you can make a specific string more generic by inserting asterisks (wildcards that replace any other characters) in the appropriate positions.

When defining Name and Publisher, select the relevant operand before entering the parameter. You can also use asterisks here, allowing the Exception to apply to other similar events.

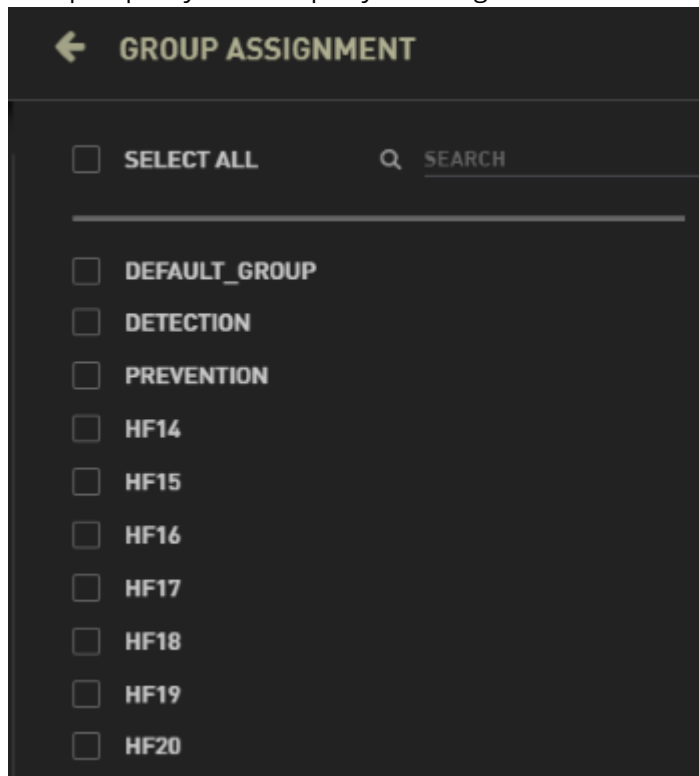
A screenshot of a configuration form titled "PARENT" with a red asterisk and "REQUIRED FIELD" label in the top right corner. The form has four input fields: "PATH", "NAME", "PUBLISHER", and "HASH". The "NAME" field is currently selected, and a dropdown menu is open below it, showing four options: "IS" (highlighted in blue), "CONTAINS", "BEGINS WITH", and "ENDS WITH".

Specify parameters for the Target (the entity impacted by the Exception), using the techniques described in Step 4. Target parameter types for most Protection Modules are **Path** and **Name**, but those for Abnormal Communication are **IP** and **Port** and those for Registry Manipulation are **Key** and **Value**.

A screenshot of a configuration form titled "TARGET". It has two input fields: "PATH" and "NAME". The "NAME" field has a dropdown menu open below it, showing the option "IS".

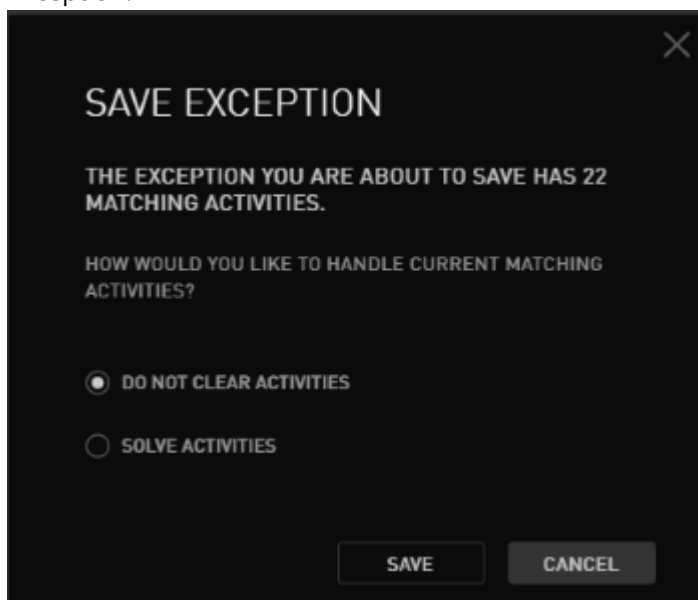
- 5.
6. By default, new Exceptions are unassigned (**Assign To None**) and do not affect event handling until they are assigned to endpoints. You can assign the Exception in one of the following ways:
 - **Assign as a default policy:** Select this radio button to add the new policy to the [Default Policy Set](#). Default policies are applied to all endpoints connected to the Detection and Response Server. In multi-server setups where servers are connected to the Controller Server, these policies are also automatically distributed to the other Detection and Response Servers in the environment as default policies.

Assign to one or more groups: Select this radio button to apply the Exception to specific Groups. Specify the Groups by selecting them from the **Group Assignment** pane that opens.



Click **Save**.

The **Save Exception** dialog opens, displaying the number of activities that match the new Exception.



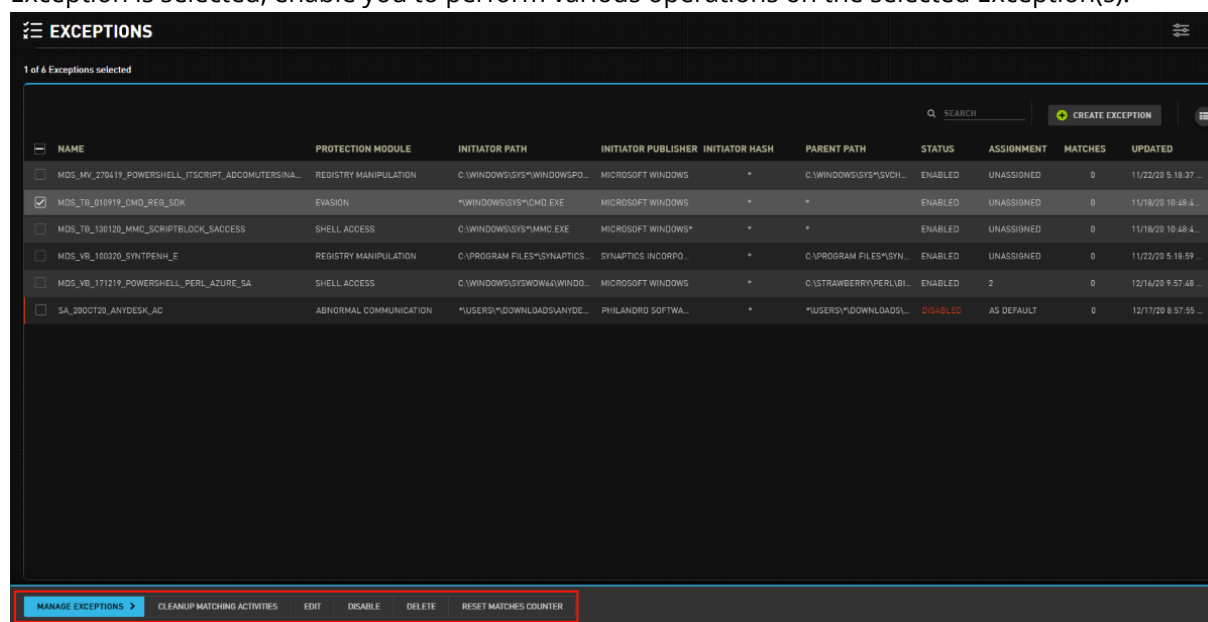
- 7.
8. Select an option for handling matching activities:
 - **Do not clear activities:** Matching activities will continue to be displayed in the Security Center.

- **Solve activities:** Matching activities will be marked as resolved and cleared from the Security Center view.

9. To close the dialog and add the new Exception to the Exceptions list, click **Save**.

Exception Management in the Detection and Response Management Console

The buttons in the lower left corner of the **Exceptions** page, which appear when at least one Exception is selected, enable you to perform various operations on the selected Exception(s).



The options are:

Action	Description
Edit	Opens a side pane in which you can view and update all parameters of a selected Exception. (This pane also opens when you click the row of an Exception.) For more information about parameters, refer to Adding Exceptions in the Detection and Response Management Console .
Enable / Disable	These actions activate and inactivate Exceptions. For details, refer to Disabling and Enabling Exceptions .
Delete	Removes Exceptions from the system. For details, refer to Deleting Exceptions .
Cleanup Matching Activities / Reset Matches Counter	These actions allow you to handle matching activities .

Disabling and Enabling Exceptions

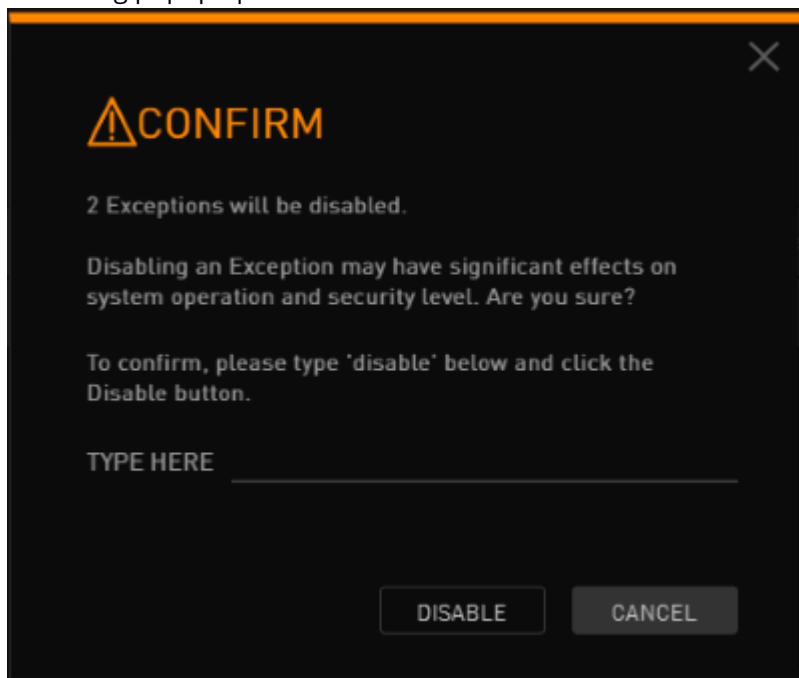
Use the Disable action when you need to temporarily inactivate one or more Exceptions.

To disable and enable Exceptions:

1. On the left side of the Exceptions grid, select the checkbox(es) of the Exception(s) that you want to disable.

From the **Manage Exceptions** action bar, click **Disable**.

A warning popup opens.



2.

Enter the word *disable* (not case sensitive) on the line provided. Then, click **Disable**.

The popup closes, and the Exceptions are labeled **Disabled** in the **Status** column.

NAME	PROTECTION MODULE	INITIATOR PATH	INITIATOR PUBLISHER	INITIATOR HASH	PARENT PATH	STATUS	ASSIGNMENT	MATCHES	UPDATED
<input type="checkbox"/> MDS_MY_270419_POWERSHELL_ITSCRIPT_ADCOMPUTERSINA...	REGISTRY MANIPULATION	C:\WINDOWS\SYS*WINDOWSPO...	MICROSOFT WINDOWS	*	C:\WINDOWS\SYS*SVCH...	ENABLED	UNASSIGNED	0	11/22/20 5:18:37 ...
<input type="checkbox"/> MDS_TB_010919_CMD_REB_SDK	EVASION	*\WINDOWS\SYS*CMD EXE	MICROSOFT WINDOWS	*	*	ENABLED	UNASSIGNED	0	11/18/20 10:48:4...
<input type="checkbox"/> MDS_TB_130120_MMIO_SCRIPTBLOCK_SACCESS	SHELL ACCESS	C:\WINDOWS\SYS*MMIO EXE	MICROSOFT WINDOWS*	*	*	ENABLED	UNASSIGNED	0	11/18/20 10:48:4...
<input type="checkbox"/> MDS_VB_100220_SYNTPEH_E	REGISTRY MANIPULATION	C:\PROGRAM FILES*\SYNAPTICS...	SYNAPTICS INCORPO...	*	C:\PROGRAM FILES*\SYN...	ENABLED	UNASSIGNED	0	11/22/20 5:18:59 ...
<input type="checkbox"/> MDS_VB_171219_POWERSHELL_PERL_AZURE_SA	SHELL ACCESS	C:\WINDOWS\SYS*WOW64\WINDO...	MICROSOFT WINDOWS	*	C:\STRAWBERRY\PERL\BI...	ENABLED	2	0	12/14/20 9:57:48 ...
<input type="checkbox"/> PESTUDIO	ABNORMAL COMMUNICATION	C:\USERS\PODESKTOP\STATIC...	*	7EC3F2B4DF2C2D...	*	DISABLED	AS DEFAULT	0	12/17/20 8:57:55 ...
<input type="checkbox"/> SA_200220_ANYDESK_AC	ABNORMAL COMMUNICATION	*\USERS*\DOWNLOADED\ANYDE...	PHILANDRO SOFTWARE	*	*\USERS*\DOWNLOADED...	DISABLED	AS DEFAULT	0	12/17/20 8:57:55 ...

3.

4. To reactivate the Exception(s), select the relevant checkbox(es) and click **Enable**.

Deleting Exceptions

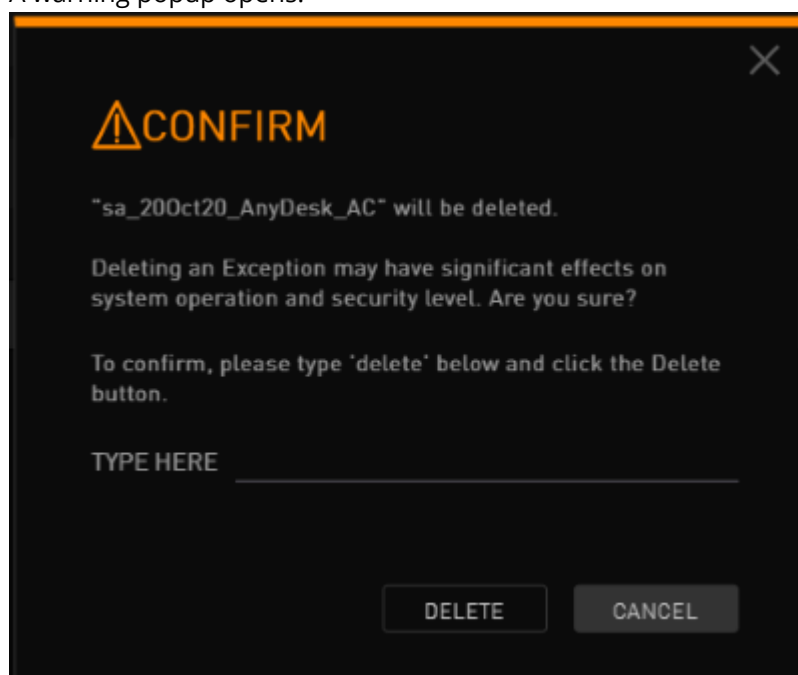
The Delete action permanently removes selected Exceptions from the system.

To delete Exceptions:

1. On the left side of the Exceptions grid, select the checkbox(es) of the Exception(s) that you want to delete.

From the **Manage Exceptions** actions bar, click **Delete**.

A warning popup opens.



- 2.
3. Enter the word *delete* (not case sensitive) on the line provided. Then, click **Delete**.
The selected Exceptions are removed from the **Exceptions** list and are deleted from the system.

Handling Matching Activities

The following actions are related to managing Exception matches:

- **Reset Matches Counter:** Zeroes the counter for the number of Endpoints on which an Exception had matches.
- **Cleanup Matching Activities:** Clears matching activities from the Security Center by solving or removing them.

Resetting the Matches Counter

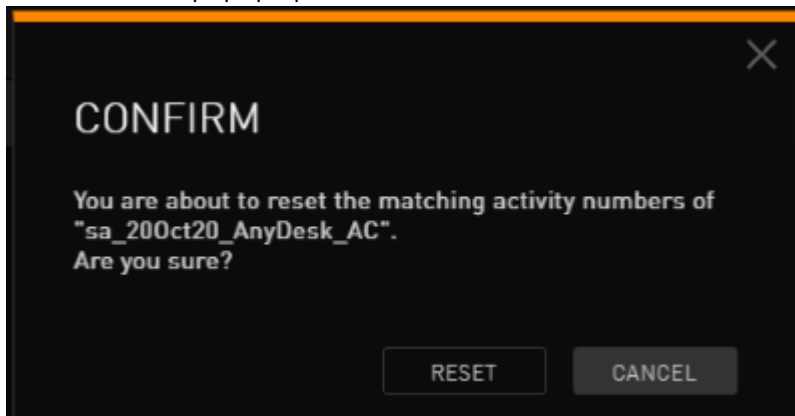
The **Matches** column of the Exceptions grid is a counter showing the number of endpoints on which the Exception had matches. The Reset Matches Counter action resets the count in this column to zero.

To reset the matches counter for an Exception:

1. At the left side of the Exceptions grid, select the checkbox of the relevant Exception.

From the **Manage Exceptions** actions bar, click **Reset Matches Counter**.

A confirmation popup opens.



2.

3. Click **Reset**.

A confirmation message is displayed, and the counter is reset to zero.

Clearing Matching Activities from the Security Center

The Cleanup Matching Activities action enables you to clear matching activities from the Security Center. You can clear activities using either of the following methods:

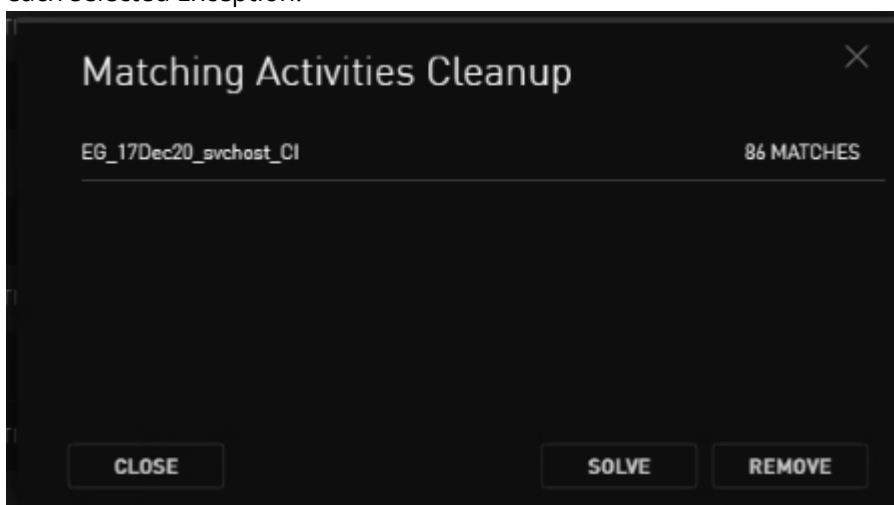
- **Solve activities:** Marks the activities as resolved and removes them from the Security Center view.
- **Remove activities:** Removes activities from the Security Center view and deletes them from the Detection and Response database.

To clear matching activities:

1. At the left side of the Exceptions grid, select the checkbox of the relevant Exception(s).

From the **Manage Exceptions** actions bar, click **Cleanup Matching Activities**.

The **Matching Activities Cleanup** dialog opens, listing the number of matching activities for each selected Exception.



2.

3. Click **Solve** or **Remove** (according to how you want to clear the activities).

A confirmation message is displayed when the process completes successfully.



4. To exit the dialog, click **Close**.

Working with Hardening Policies

Hardening Policies: Overview

In contrast to Exceptions, which allow processes that the BPM analysis technique normally denies, Hardening Policies deny processes that would normally be allowed. Hardening Policies (HPs) provide a means for organizations to regulate internal application usage and control internal access to their high-value Assets.

Hardening Policies work through application control, a method which permits or blocks processes that are attempting to access system resources on an endpoint. You can use application control to determine which processes can run on endpoints, block communication with unwanted destinations, and much more.

Some use cases for applying HPs include:

- Blocking internal use of unwanted applications (such as Dropbox or Skype)
- Preventing users from changing configuration files
- Controlling access to specific registry keys
- Limiting access to particular folders

Defining Hardening Policies in the Detection and Response Management Console

HPs can be defined for both workstations and servers, and can be as specific or as broad as necessary. The general aim of a HP is set according to the option selected in these parameters:

- **Mode:**
 - **Alert:** When the policy is violated, the prohibited operation is allowed, and a Hardening Policy Violation event is triggered.
 - **Block:** When the policy is violated, the prohibited operation is prevented, and a Hardening Policy Violation event is triggered.
- **Operation:** A Hardening Policy can focus on any aspect of ONE of the following operations:
 - **Filesystem access:** Involves access rights (read, write or both) to specified folders or files.
 - **Process execution:** Involves definition of Initiators that are allowed to execute specific processes.
 - **Network access:** Involves access to specified IP/ports.
 - **Registry access:** Involves access rights (read, write or both) to specified registry keys.

The specific purpose of a HP is determined by the parameters defined in the Initiator and Target settings of the policy. A Hardening Policy can support multiple values for both Initiators and Targets.

The following sections provide more details about working with Hardening Policies:

- [Working with the Hardening Policies Set](#)
- [Understanding Hardening Policy Parameters](#)
- [Adding Hardening Policies to Your HP Set](#)
- [Assigning Hardening Policies to Groups](#)

Working with the Hardening Policies Set

Since every Hardening Policy (HP) is individualized according to organizational needs, each company builds its own unique set of HPs. (There are no out-of-the-box HPs.) The HP set is displayed on the **Hardening Policies** page of the Detection and Response Management Console.

The following sections present:

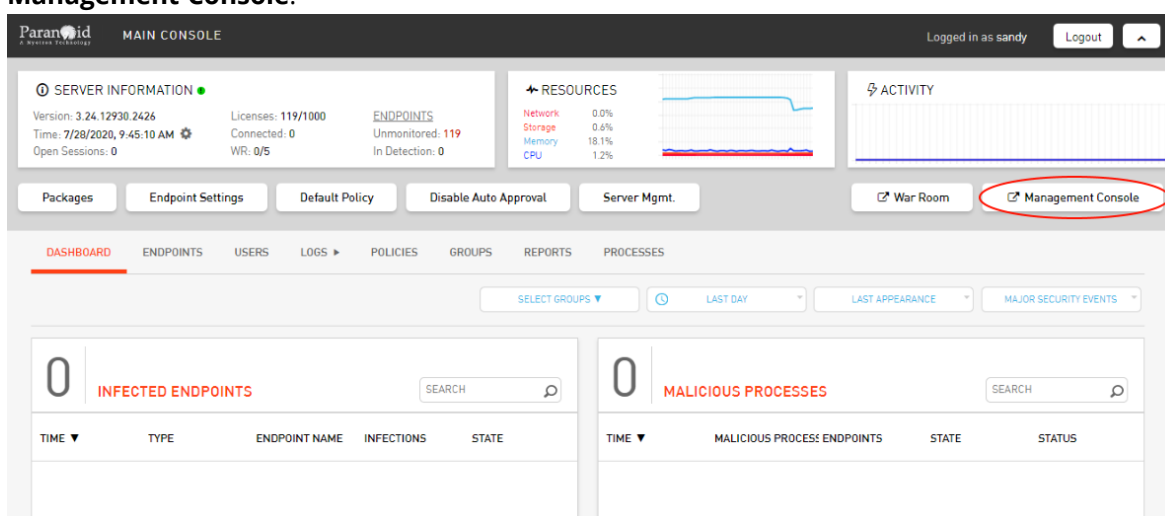
- [Accessing the HP Page](#)
- [Viewing and Managing the HP List](#)

Accessing the HP Page

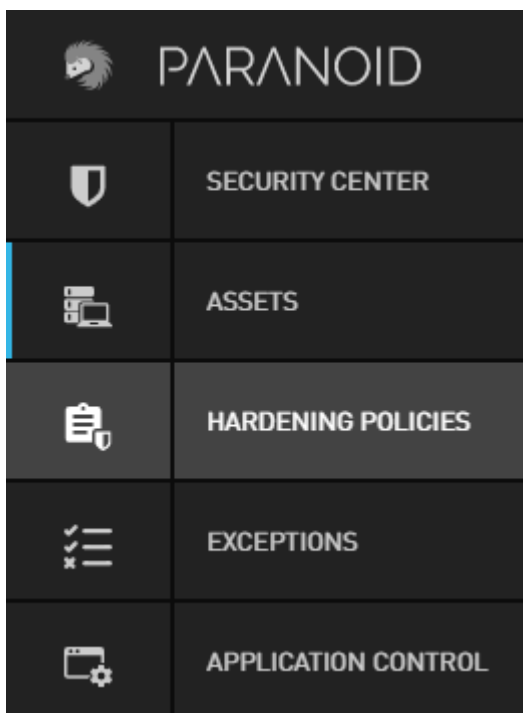
The **Hardening Policies** page is part of the new Detection and Response Management Console.

To access the HP page:

At the upper right side of the Detection and Response Monitoring Environment, click **Management Console**.



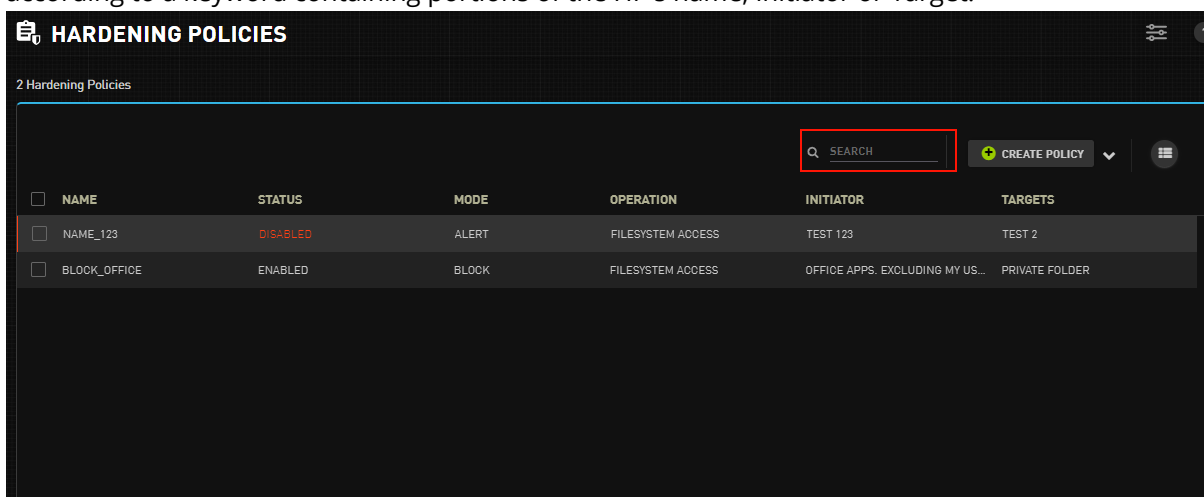
1. The Detection and Response Management Console opens in a new browser tab, with the Security Center view displayed.
2. At the left side of the Detection and Response Management Console, hover over the menu bar to open it, and select **Hardening Policies**.



The **Hardening Policies** page opens, listing any HPs that have been created.

Viewing and Managing the Hardening Policies List

The **Hardening Policies** page lists the HPs that have been created and provides general information about each one. The Search tool at the top of the page enables you to filter the list according to a keyword containing portions of the HP's name, Initiator or Target.

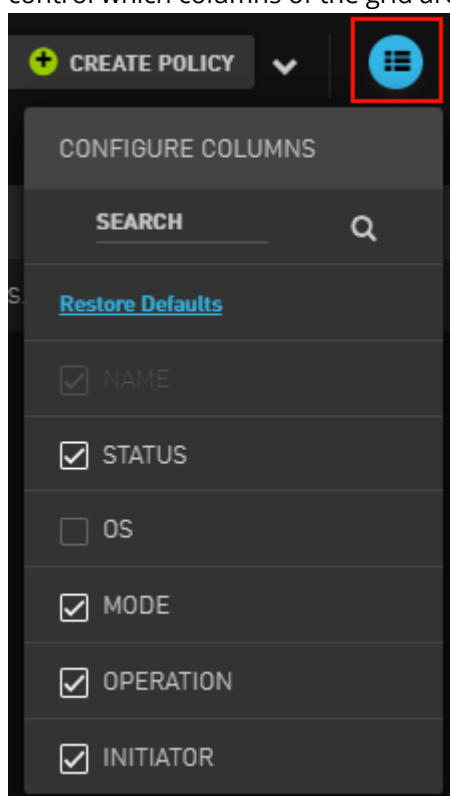


The following data is displayed in the HP grid:

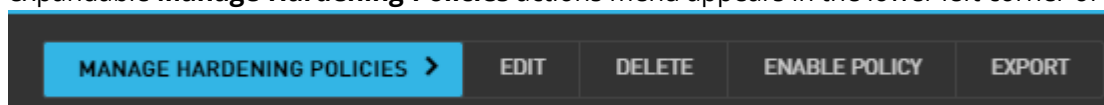
Column	Description
Name	The user-assigned name of the HP.
Status	<ul style="list-style-type: none"> Enabled: The HP is currently active. Disabled: The HP has been inactivated. Disabled HPs are indicated by red font in the Status column, and a red bar at the left side of the row.

Column	Description
Mode	<ul style="list-style-type: none"> • Alert: When the policy is violated, the operation is permitted. • Block: When the policy is violated, the operation is prevented. <p>In either mode, a violation of the HP generates an event in the Detection and Response Monitoring Environment. Depending on Agent configuration, an alert may also be displayed on the endpoint.</p>
Operation	The category of operation affected by the HP (Filesystem access, Process execution, Network access or Registry access).
Initiator	The user-assigned description for the Initiator.
Targets	The user-assigned description for the Target(s).

Clicking the Columns icon (in the upper right corner of the grid) opens a popup that allows you to control which columns of the grid are displayed.



When one or more HPs are selected (by checking the checkbox to the left of the name), the expandable **Manage Hardening Policies** actions menu appears in the lower left corner of the page.

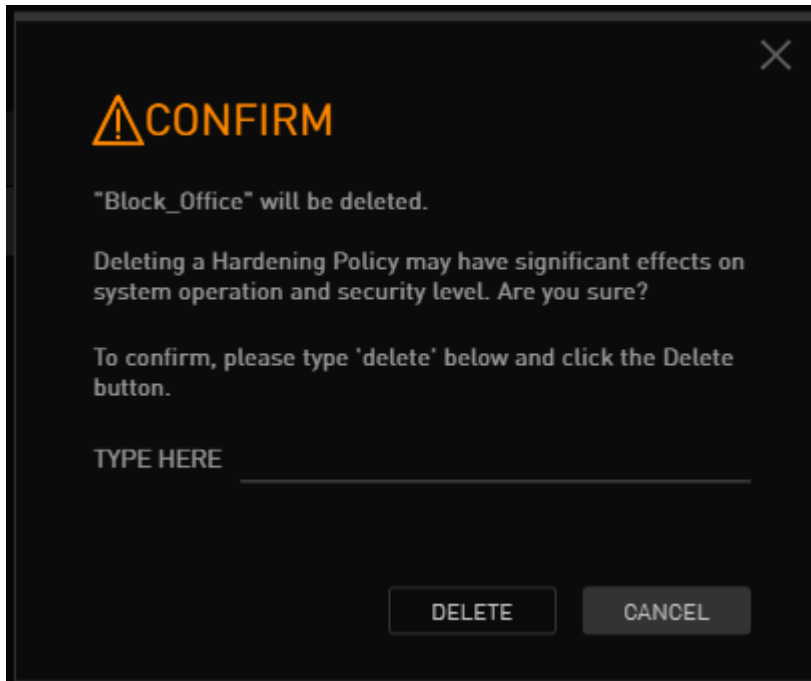


The following actions are available:

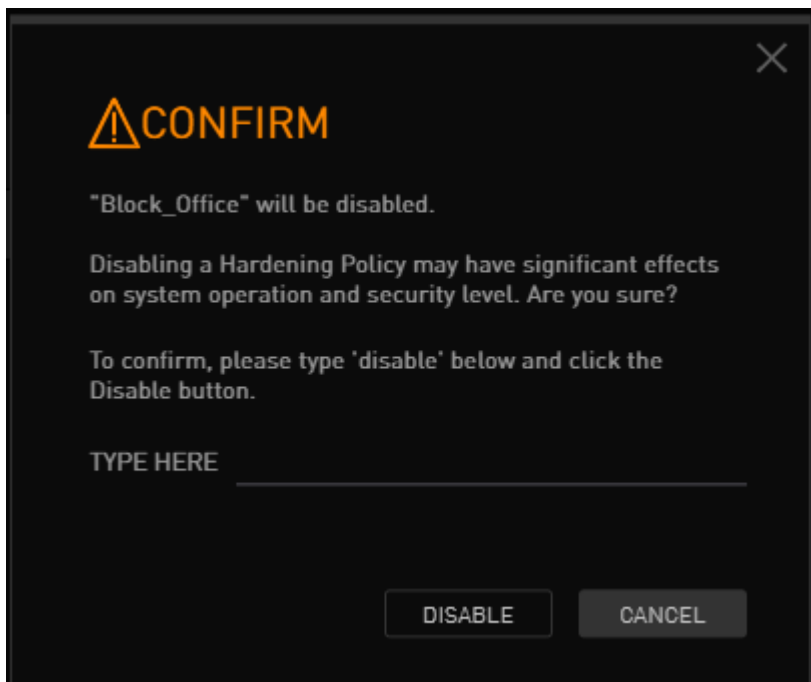
- **Edit:** Opens a side panel where you can view and update parameters of the selected HP (if multiple HPs are selected, the Edit action is hidden). You can also open this panel by clicking the relevant row of the HP grid. For more information about editing HPs, refer to [Understanding](#)

Hardening Policy Parameters.


Delete: Allows you to remove the selected HP(s) from the system. To avoid inadvertent deletion of HPs, clicking this button opens a confirmation popup in which you need to enter the word *delete* (not case sensitive) and then click **Delete**.



Enable / Disable Policy: Allows you to activate currently disabled HPs or inactivate ones that are currently enabled. To avoid inadvertent actions, clicking this button opens a confirmation popup in which you need to enter the word *disable* or *enable* (not case sensitive) and then click the button below.



- **Export:** Allows you to download the selected HP(s) in CSV format.

Clicking  (in the upper right corner of the page) lets you design and add a new HP. For details, refer to [Adding Hardening Policies](#).

Understanding Hardening Policy Parameters

A Hardening Policy is made up of the following groups of parameters:

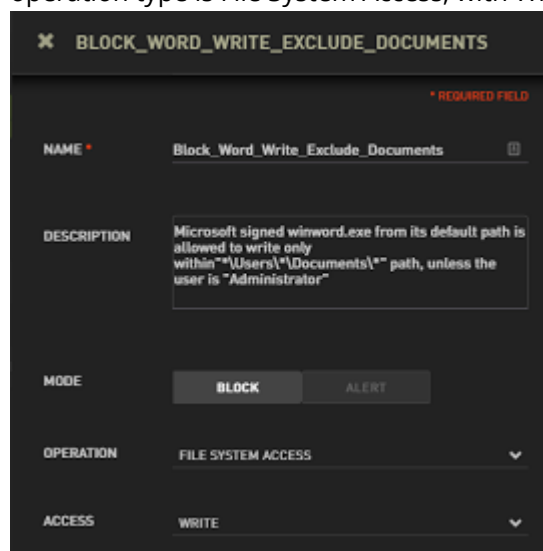
- **General parameters:** Specify the HP's name, description, operation type, and other high level determining factors.
- **Initiator parameters:** Specify details about the entities that are prohibited from performing operations on the Target.
- **Target parameters:** Specify details about the entities that are the objects of the operations performed by the Initiator.

The following sections explain more about the different types of parameters using a specific HP as a use case example.

Use Case Summary

The aim of the sample HP presented below is to limit write access to Microsoft Word documents. The HP specifies that users may write only to Word files that are located in a specific directory (the path defined in the Target parameters). Users who have Admin privileges are excluded from the HP, and they may write to Word files located in any folder.

The general parameters of the HP are shown in the figure below. Note the description, which helps other users to quickly grasp the purpose of the HP. Consistent with the logic of the HP, the operation type is File System Access, with Write access selected.



The screenshot shows a configuration form for a Hardening Policy titled "BLOCK_WORD_WRITE_EXCLUDE_DOCUMENTS". The form includes the following fields:

- NAME:** Block_Word_Write_Exclude_Documents (marked as a required field).
- DESCRIPTION:** Microsoft signed winword.exe from its default path is allowed to write only within "\\Users*\\Documents*" path, unless the user is "Administrator".
- MODE:** BLOCK (selected) and ALERT (available).
- OPERATION:** FILE SYSTEM ACCESS (selected from a dropdown menu).
- ACCESS:** WRITE (selected from a dropdown menu).

Initiator and Target Parameters

The sections below explain the types of Initiator and Target parameters available, and provides examples based on the use case presented above.

Note

When creating or updating a HP, remember that the Cartesian product of Initiator **and** Target parameters cannot exceed **25**. Calculate this product by multiplying the sums of the number of items in each parameter type. For example presented below, the Cartesian product of the HP above is 1. (There are four parameter types - 3 Initiator and one Target - but only one parameter is defined for each type. The product is therefore 1 x 1 x 1 x 1.)

Initiator Parameters

When defining the Initiator, a description plus at least one additional parameter are required. The types of initiator parameters available are identical for all HPs, regardless of operation type. The parameter types are:

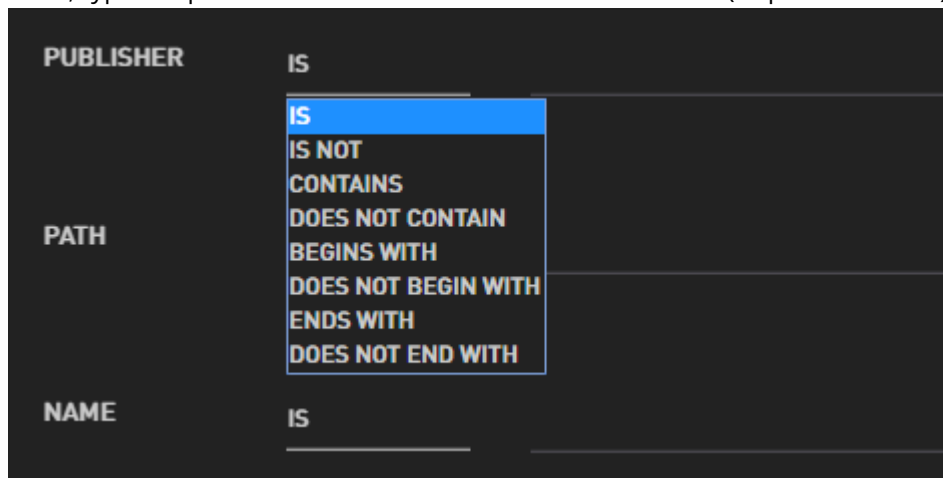
- **HASH:** The MD5 identifier of the Initiator.
- **Publisher:** The company or organization that digitally signed the Initiator.
- **Path:** File path of the Initiator.
- **Name:** Process name of the Initiator.
- **Command Line:** The executed command line of the Initiator.
- **User:** The username of the user affected by the policy.

You may define values for all the types or only some of them, according to the nature of the HP. You can also specify multiple values within the same parameter type. In runtime, the HP operates according to AND logic among the different Initiator parameter types. However, multiple values *within* a type are handled using OR logic.

To set a HASH parameter, enter the value on the line. Then, click the Add icon, or press **<Enter>**.

A dark-themed interface showing a label 'HASH' on the left. To its right is a horizontal input field. At the end of the input field is a small square button containing a plus sign (+), which is highlighted with a red rectangular border.

To set other parameter types, first select the required operator (if relevant) from the dropdown list. Then, type the parameter on the line and click the Add icon (or press **<Enter>**).

A dark-themed interface for configuring initiator parameters. It shows three rows, each with a parameter label on the left and an operator in the middle. The first row has 'PUBLISHER' and 'IS'. The second row has 'PATH' and a dropdown menu that is open, showing a list of operators: 'IS' (highlighted in blue), 'IS NOT', 'CONTAINS', 'DOES NOT CONTAIN', 'BEGINS WITH', 'DOES NOT BEGIN WITH', 'ENDS WITH', and 'DOES NOT END WITH'. The third row has 'NAME' and 'IS'. Each parameter label is followed by a horizontal input field.

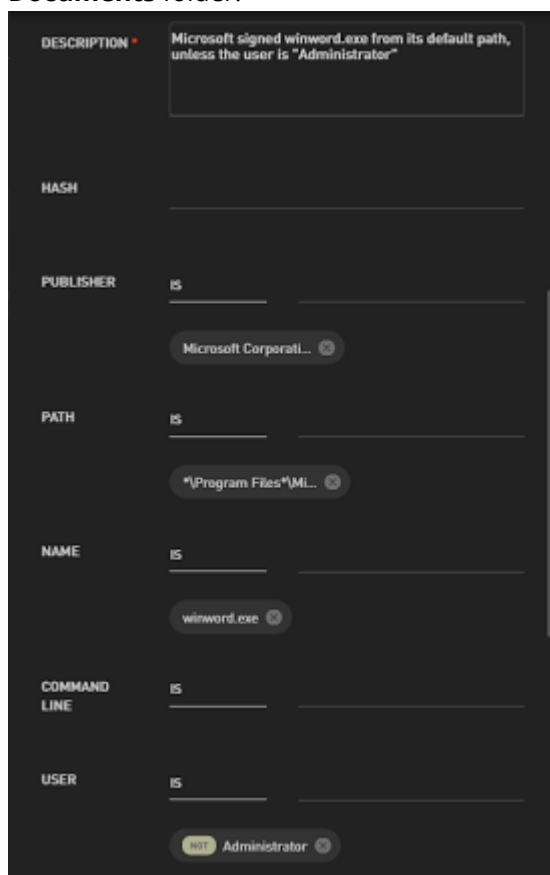
After clicking the Add icon or pressing **<Enter>**, the value is added as a chip below the input field. To add more values, repeat the process.

Note

To save Initiator parameters in the system, you need to click **Save**.

Initiator parameters for the example presented above are shown in the following figure. In this case, the Initiator's Publisher and Name are specified explicitly, while the Path is defined with a regular expression. The regular expression, which is indicated by the asterisk before **\Program Files**, specifies that all paths containing the phrase **Program Files** that lead directly to **Microsoft Office > Office 16** should be included in the logic.

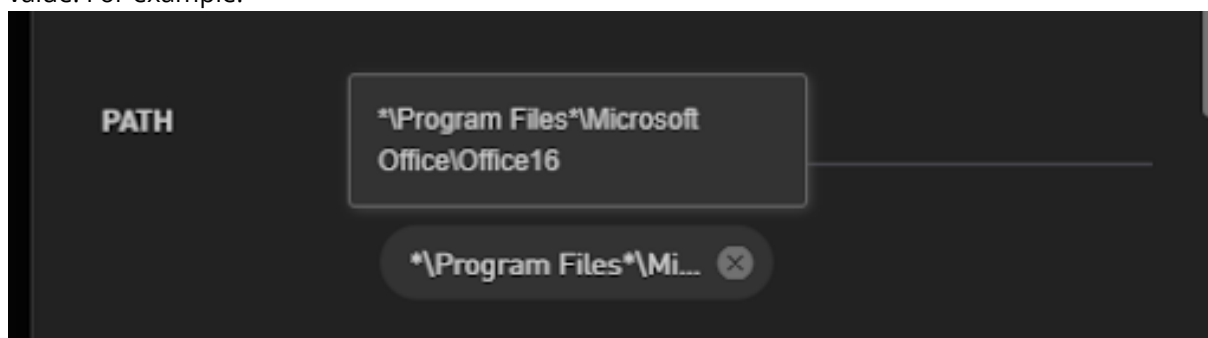
To ensure that Admin users will not be affected by the HP, a *User* parameter of **NOT Administrator** is defined. All other users will be blocked from writing to Word documents outside of the **Documents** folder.



The screenshot shows a configuration window for an Initiator. It has a dark background with white text. The parameters and their values are as follows:

Parameter	Value
DESCRIPTION	Microsoft signed winword.exe from its default path, unless the user is "Administrator"
HASH	
PUBLISHER	Microsoft Corporati...
PATH	*\Program Files*\Mi...
NAME	winword.exe
COMMAND LINE	
USER	NOT Administrator

Hovering over an Initiator parameter with a longer string opens a tooltip that displays the entire value. For example:



Target Parameters

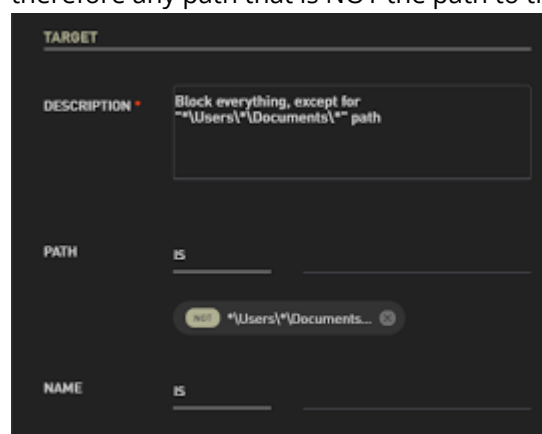
Target parameter types for most HP operations are Path and Name. HPs with an operation type of Network Access have Target parameter types of IP and Port.

As with Initiator parameters, you may define values for one or both parameter types, and multiple values can be specified within a type. If you define parameters for both Path and Name (or both IP and Port), the HP is implemented only if both parameters are matched. Multiple values specified *within* a parameter type are handled using OR logic.

Note

When adding Target parameters, be sure to click the Add icon or press **<Enter>** after typing the value of the parameter, or the system will not display the inserted value. To save Target parameters in the system, you need to click **Save**.

As described in the use case example above, the purpose of the HP is to block users from writing to any Word documents, for those that are located in the *except Documents* folder. The Target path is therefore any path that is NOT the path to that folder.



Adding Hardening Policies to Your HP Set

You can add HPs to your environment by either importing them from another Detection and Response environment, or manually creating them. The following sections provide details and guidelines for both methods:

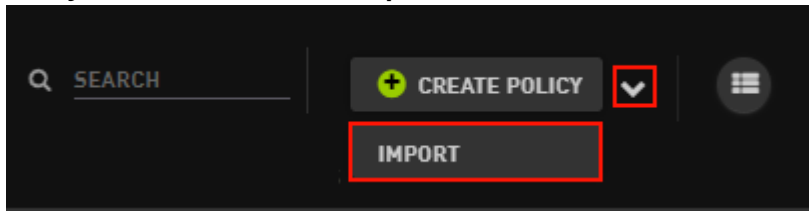
- [Importing Hardening Policies](#)
- [Creating Hardening Policies: General Guidelines](#)

Importing Hardening Policies

The Import function enables you to add HPs from another Detection and Response environment to your set of HPs.

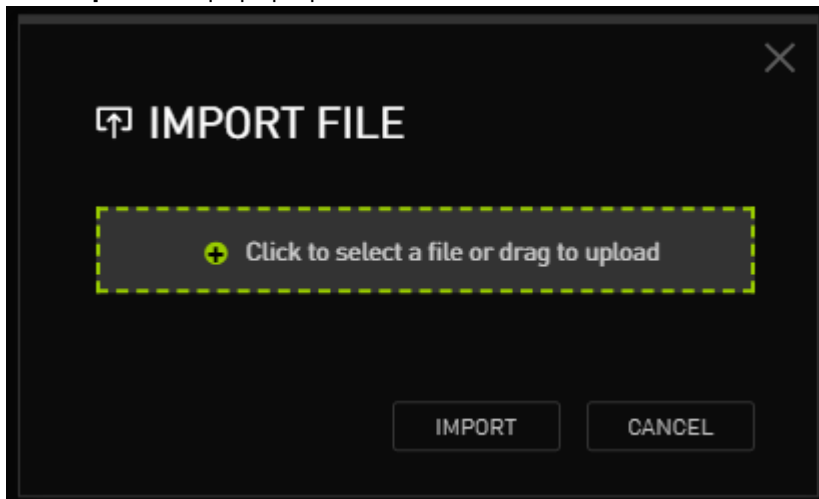
To import Hardening Policies:

In the upper right corner of the **Hardening Policies** page, click the carat next to the **Create Policy** button and then click **Import**.



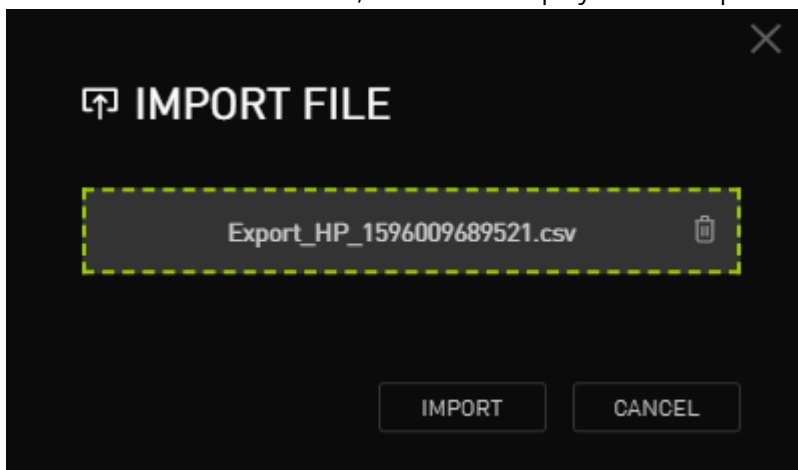
1.

The **Import File** popup opens.



Drag-and-drop the relevant file to the upload area. Alternatively, click in the upload area. Then, navigate to and select the file.

Once a file has been selected, its name is displayed in the upload area.



2.

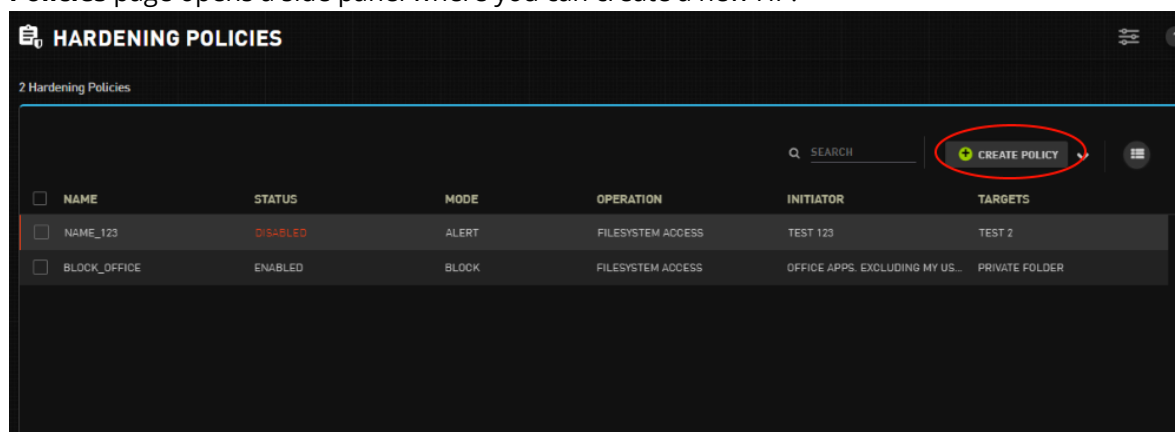
3. Click **Import**.

The imported HPs are listed on the **Hardening Policies** page, and a confirmation message is displayed at the top of the page.

General Guidelines for Creating and Updating Hardening Policies

When manually adding new HPs (or updating existing ones), keep the following guidelines and recommendations in mind:

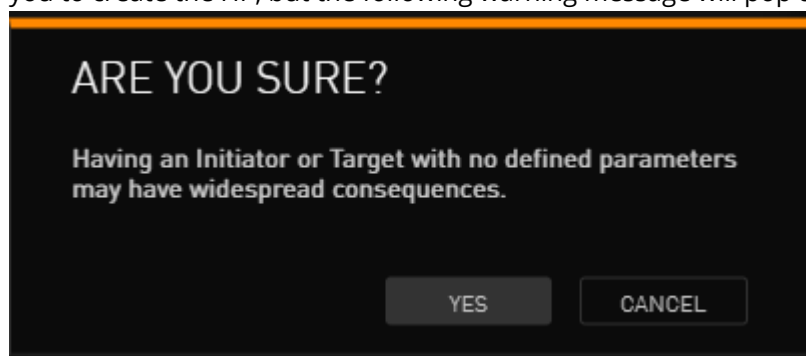
Creating a HP: Clicking the **Create Policy** button in the upper right corner of the **Hardening Policies** page opens a side panel where you can create a new HP.



- **Naming your HP:** Each HP must have a unique name. It is recommended to assign a name that is relevant to the purpose of the HP. Names may contain letters, numbers and underscores only (no special characters), and may be no longer than 100 characters.
- **Description fields:** A description for the HP is not mandatory but is recommended. Descriptions are required for both the Initiator and the Target.

Initiator/Target parameters: To create a HP, you must define at least one parameter for *either* the Initiator or the Target (in addition to the Description), and it is strongly recommended to specify at least one parameter for both. If you define one or more parameters for the Initiator but none for the Target (or vice versa), the Detection and Response Management Console will allow

- you to create the HP, but the following warning message will pop up when you click **Save**:



- **Number of parameters:** The Cartesian product of Initiator **and** Target parameters in a Hardening Policy cannot exceed **25**. Calculate this product by multiplying the sums of the number of items in each parameter type. For example, a policy has two Initiator types (Path and Name), containing one value each. The Target parameter types of Path and Name each contain 2 values each. The Cartesian product is therefore $1 \times 1 \times 2 \times 2 = 4$.)
- **Saving changes:** Be sure to click **Save** after creating or updating a HP. If you close the panel before saving, any changes will be lost.
- **Updating a HP:** Once you have added a HP, you can update any of its parameters by selecting the policy from the HP list, modifying the relevant parameters in the side panel that opens, and clicking **Save**. If you open the side panel inadvertently, or you want to discard changes, close the

panel by clicking the Close icon at the top, or the **Cancel** button at the bottom.

BLOCK_OFFICE

* REQUIRED FIELD

NAME * Block_Office

DESCRIPTION Block Office apps from writing to a private folder

MODE BLOCK ALERT

OPERATION FILE SYSTEM ACCESS

ACCESS WRITE

INITIATOR

DESCRIPTION * Office Apps. Excluding my user.

HASH

SAVE CANCEL

Specifying HP General Parameters

Use the following procedure to define the general parameters for your HP.

To specify general parameters for a HP:

1. At the top of the **Hardening Policy** panel, enter a logical name for the HP. The name may contain letters, numbers and underscores only (no special characters), and can be no longer than 100 characters.

HARDENING POLICY

* REQUIRED FIELD

NAME *

DESCRIPTION

MODE

BLOCK ALERT

OPERATION FILE SYSTEM ACCESS

ACCESS ALL

2. In the **Description** field, it is recommended to enter a brief summary of the purpose of the HP.
3. Select a Mode for your HP. The default mode of a new HP is **Alert**. In this mode, you receive notifications about operations prohibited by the HP, but the operations themselves continue to take place. In **Block** mode, operations prohibited by the HP are prevented.

From the **Operation** dropdown, select the relevant operation type for the HP. The default operation type is File System Access.

OPERATION PROCESS EXECUTION

FILE SYSTEM ACCESS

NETWORK ACCESS

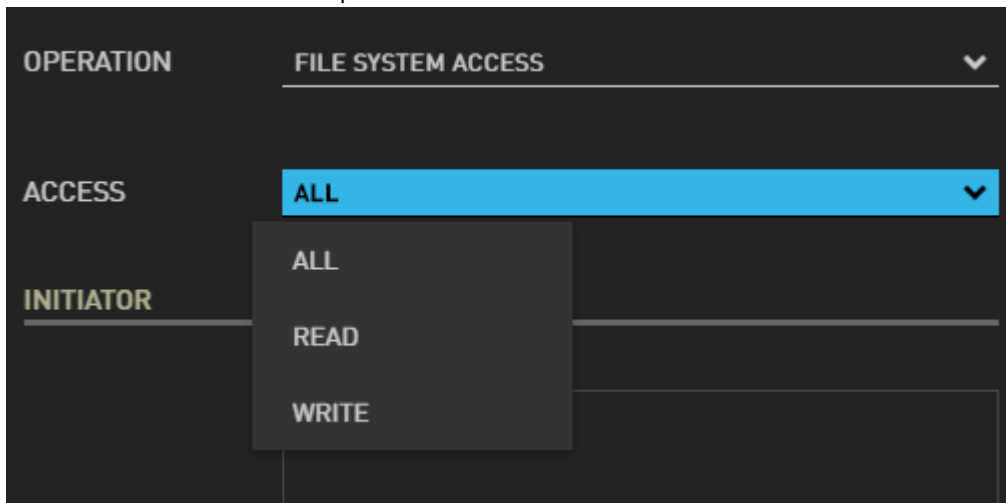
PROCESS EXECUTION

REGISTRY ACCESS

INITIATOR

4.

If you selected **File System Access** or **Registry Access** in Step 4, select the relevant type of access from the **Access** dropdown.

A screenshot of a configuration interface with a dark theme. It shows a form with three sections: 'OPERATION' with a dropdown set to 'FILE SYSTEM ACCESS', 'ACCESS' with a dropdown set to 'ALL', and 'INITIATOR' which is currently empty. The 'ACCESS' dropdown is open, showing a list with 'ALL' at the top, followed by 'READ' and 'WRITE'.

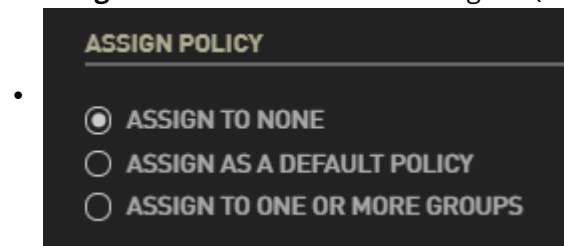
- 5.
6. Continue by defining parameters for the Initiator and the Target. Refer to [Understanding Hardening Policy Parameters](#) for more information.

Assigning Hardening Policies to Groups

Like Exceptions, Hardening Policies (HPs) do not have any impact until they are assigned to one or more Groups. Administrators need to assign HPs manually. By default, HPs are not assigned.

The **Assign Policy** frame allows you to assign a HP to relevant Groups. This frame is located at the bottom of the settings pane that opens when creating or editing a HP. The following assignment options are available:

Assign to None: The HP is not assigned (default option).

A screenshot of the 'ASSIGN POLICY' frame. It has a title 'ASSIGN POLICY' and three radio button options: 'ASSIGN TO NONE' (which is selected), 'ASSIGN AS A DEFAULT POLICY', and 'ASSIGN TO ONE OR MORE GROUPS'.

- **Assign as a Default Policy:** The HP is assigned to all Assets. Select this option only if the HP is relevant to *all* endpoints.

To assign the HP as a Default Policy, select the radio button and then click **Save**.

- **Assign to One or More Groups:** The HP is assigned to specific selected endpoints Groups. Use this option to assign HPs that affect only a portion of your Assets.

When a HP is assigned to selected Groups, the name(s) of the Group(s) to which it is currently assigned is displayed below the radio button, and the **Edit** link allows you to quickly update the Group assignments. (Refer to the procedure below for more details.)

ASSIGN POLICY

☐ ASSIGN TO NONE

☐ ASSIGN AS A DEFAULT POLICY

☒ ASSIGN TO ONE OR MORE GROUPS

Servers [Edit](#)

To assign a Hardening Policy to specific Groups:

From the **Hardening Policies** page, click the relevant HP to open the settings pane. At the bottom of the pane, under **Assign Policy**, select the **Assign to One or More Groups** radio button. If the radio button is already selected, click **Edit**.

A side panel opens, listed all defined Groups.

BLOCK_OFFICE **GROUP ASSIGNMENT**

USER IS

NOT Shai

TARGET

DESCRIPTION Private Folder

PATH IS

C:\Users\shai\Docum...

NAME IS

ASSIGN POLICY

☐ ASSIGN TO NONE

☐ ASSIGN AS A DEFAULT POLICY

☒ ASSIGN TO ONE OR MORE GROUPS

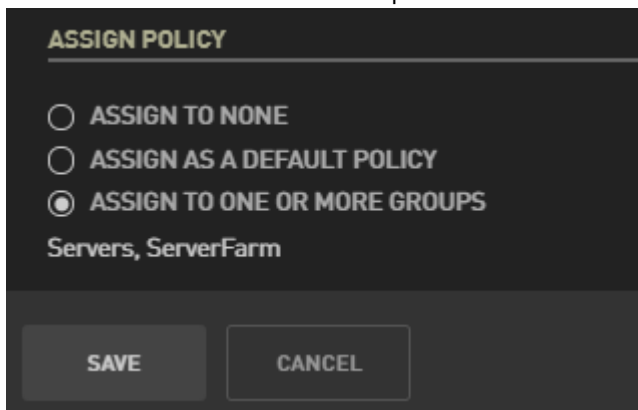
SAVE CANCEL

SELECT ALL SEARCH

- ☐ DEFAULT_GROUP
- ☐ MEDIUM_RISK
- ☐ HIGH_RISK
- ☐ LOW_RISK
- ☐ SERVERS
- ☐ PREVENTION
- ☐ MYDEMOGROUP
- ☐ SERVERFARM
- ☐ RMS_DETECTION
- ☐ RMS_DISARM

- 1.
2. Specify the Group(s) to which you want to assign the HP by selecting the relevant checkbox(es). To quickly find a Group, filter the list by entering part or all of the Group's name in the **Search** field (above the list).

The names of the selected Groups are listed in the **Assign Policy** frame.



ASSIGN POLICY

☐ ASSIGN TO NONE

☐ ASSIGN AS A DEFAULT POLICY

☒ ASSIGN TO ONE OR MORE GROUPS

Servers, ServerFarm

SAVE **CANCEL**

3. Click **Save**.

The panes close, and the HP is assigned to the selected Group(s).

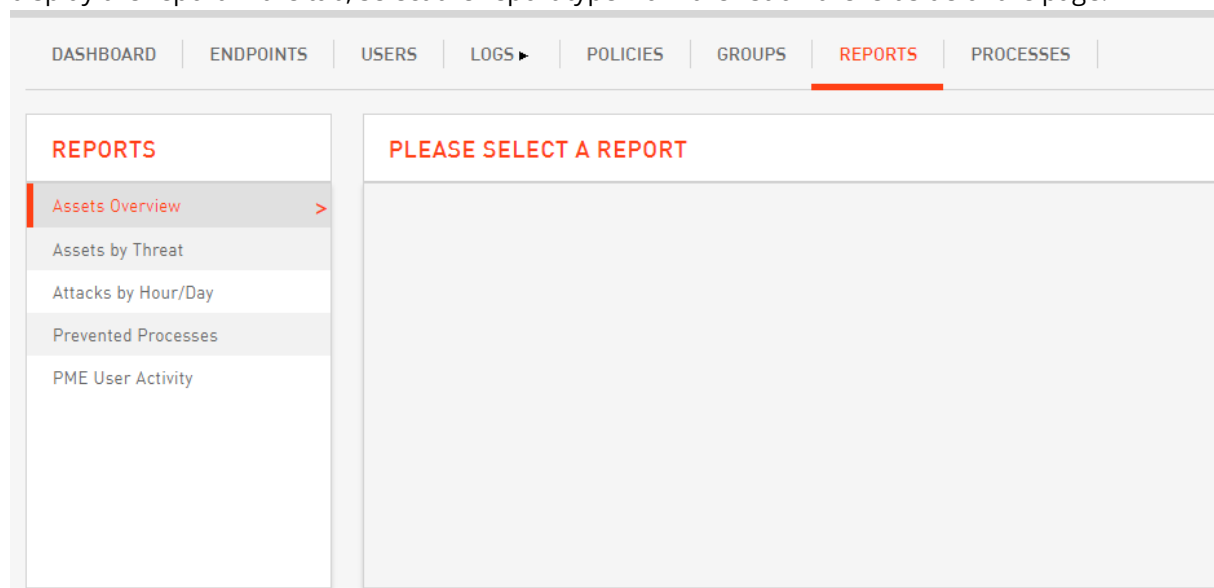
Handling Administrative Operations

Viewing Detection and Response Monitoring Environment Reports

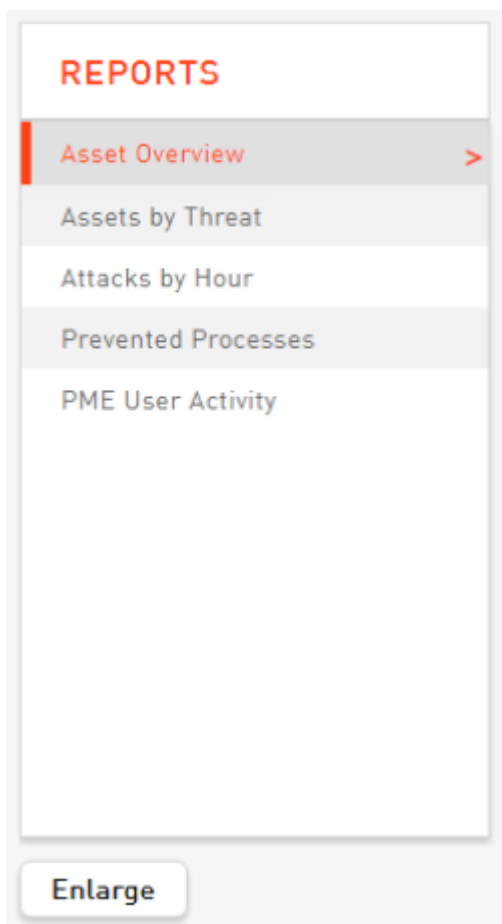
The Detection and Response Monitoring Environment reports provide a snapshot view of your environment, so you can quickly check the status of assets and users. The reports are:

- [Assets Overview](#): Lists all endpoints and servers and provides general information about each one.
- [Assets by Threat](#): Provides a summary of all assets that have been infected during the past day.
- [Attacks by Hour/Day](#): Shows the average number of attacks during a selected time period.
- [Prevented Processes](#): Lists the processes whose activities were most recently prevented by Detection and Response.
- [Detection and Response Monitoring Environment User Activity](#): Displays the number of users and shows a breakdown of user activities according to activity type.

To view a report, click the **Reports** tab of the Detection and Response Monitoring Environment. To display the report in the tab, select the report type from the list on the left side of the page.



Once a report is displayed, you can click the **Enlarge** button (at the lower left corner of the page) to open it in a popup window.



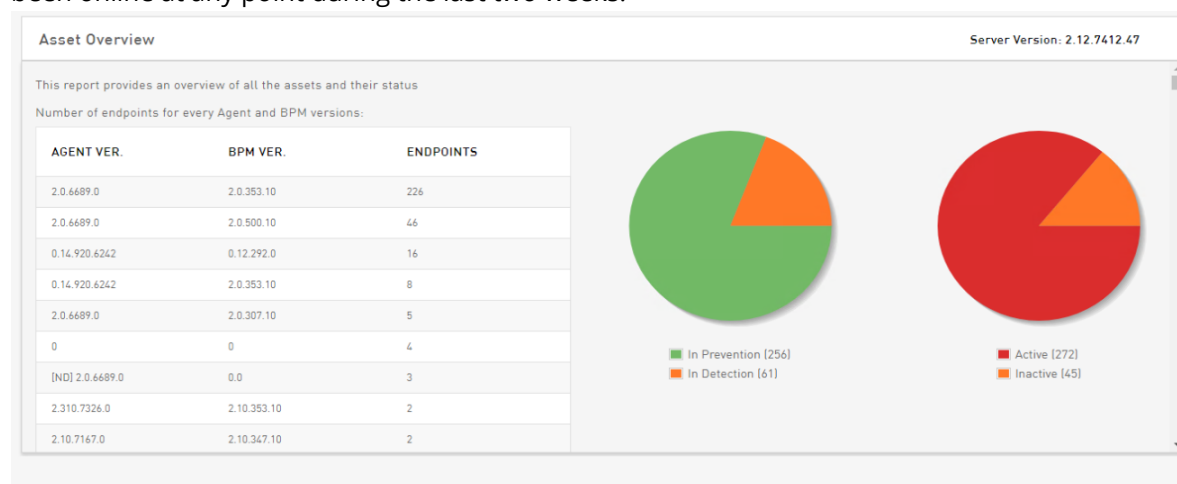
The following sections describe each report in more detail.

Assets Overview

This report provides a summary of all assets (endpoints and servers). The upper portion of the report shows the total number of endpoints according to the following breakdowns:

- **Agent and BPM Version:** Number of endpoints on which specific Agent/BPM versions are installed.
- **Mode:** Number of endpoints in Prevention Mode and number of endpoints in Detection Mode.

Activity: Number of Active and Inactive (offline) endpoints. Active endpoints are those that have been online at any point during the last two weeks.



The lower portion of the report displays the Detailed Assets List. This grid lists all the endpoints (in alphabetical order according to endpoint name). Additional information provided includes IP, Mode, Agent/BPM version, Groups to which the endpoint is assigned, and number of days that the endpoint has been offline (if relevant).

ENDPOINT	IP	GROUP(S)	MODE	OFFLINE FOR (DAYS)	AGENT VER.	BPM VER.
ADAM-LPT	172.21.1.130	QA	Detection	28	2.10.7167.0	2.10.346.0
ADIL-PC	172.21.1.96	Other_Group	Prevention	28	2.10.7167.0	2.10.346.0
ALEX-PC	172.21.1.124	Other_Group	Prevention	27	2.10.7167.0	2.10.346.0
ALEXANDRA-PC	172.21.1.126	Other_Group	Prevention	28	2.10.7167.0	2.10.346.0
AMICHAJ-PC	172.21.1.198	Other_Group	Prevention	32	2.10.7167.0	2.10.346.0
AMIR-LPT	172.21.1.164	Other_Group	Prevention	42	2.0.6759.0	2.0.343.0
AMIT-LPT	172.21.1.161	Amit	Prevention	28	2.13.7274.0	2.10.347.0
emit-lpt	172.21.1.161	Amit	Prevention	28	0	0
ARKADY-PC	192.168.1.137	Other_Group	Prevention	59	2.10.6611.0	2.10.334.0
ARTHUR-PC	172.21.1.140	Other_Group	Prevention	61	2.10.6611.0	2.10.334.0
BRASIL-PC	172.21.1.173	SecureBoot	Prevention	102	0.20.6488.2	0.0
CHAK-PC	172.21.1.156	Other_Group	Prevention	28	2.10.7167.0	2.10.346.0
DANIEL-PC	172.21.1.160	Other_Group	Prevention	116	2.0.6197.0	2.0.297.0
DC2012-2	172.21.1.66	Other_Group	Prevention	28	2.10.6611.0	2.10.334.0
DESKTOP-MSKLVK6	192.168.1.154	US_Office	Prevention	48	2.0.6759.0	2.0.343.0

Assets by Threat

This report provides a summary of all assets that have been infected during the last 24 hours. The grid at the top shows the following information:

- **Infected Endpoints:** Total number of infected endpoints, with a breakdown according to Mode.
- **Infected Groups:** Total number of Groups that contain infected endpoints.
- **Malicious Processes:** Total number of processes involved in endpoint infections.

The lower portion of the report displays the Detailed Infected Assets List. This grid lists all the endpoints that have been infected. Additional information provided includes IP, Mode, Agent/BPM version, total number of infections and the timestamp of the most recent infection.

Assets by Threat

Server Version: 2.13.7081.94

This report provides an overview of all infected assets (last 24 hours) and related threats.

INFECTED ENDPOINTS			INFECTED GROUPS	MALICIOUS PROCESSES
IN DETECTION	IN PREVENTION	TOTAL		
6	6	12	5	18

Detailed Infected Assets List

ENDPOINT	IP	MODE	AGENT VER.	BPM VER.	LAST INFECTION	TOTAL INFECTIONS
DONNA-PC	192.168.16.91	Prevention	0.14.500.4206	0.14.246.0	2017-06-03 12:44:28	2
IDO-LPT	192.168.16.119	Detection	0.14.500.4206	0.14.246.0	2017-05-13 16:51:32	1
DAN-LPT	192.168.16.185	Detection	0.14.500.4206	0.14.246.0	2017-05-19 11:04:03	1
INTERGRATOR-PC	192.168.19.136	Prevention	0.14.500.4206	0.14.246.0	2017-06-17 09:34:02	1
IT-PC	192.168.17.102	Prevention	0.14.500.4206	0.14.246.0	2017-06-14 10:18:49	1
TERMINAL-PC	192.168.1.82	Prevention	0.14.500.4206	0.14.246.0	2017-06-25 23:45:03	1
CISO-LPT	192.168.19.134	Prevention	0.14.500.4206	0.14.246.0	2017-06-01 18:49:29	1
CONFERENCE-PC	192.168.16.80	Detection	0.14.500.4206	0.14.246.0	2017-05-10 07:44:02	1

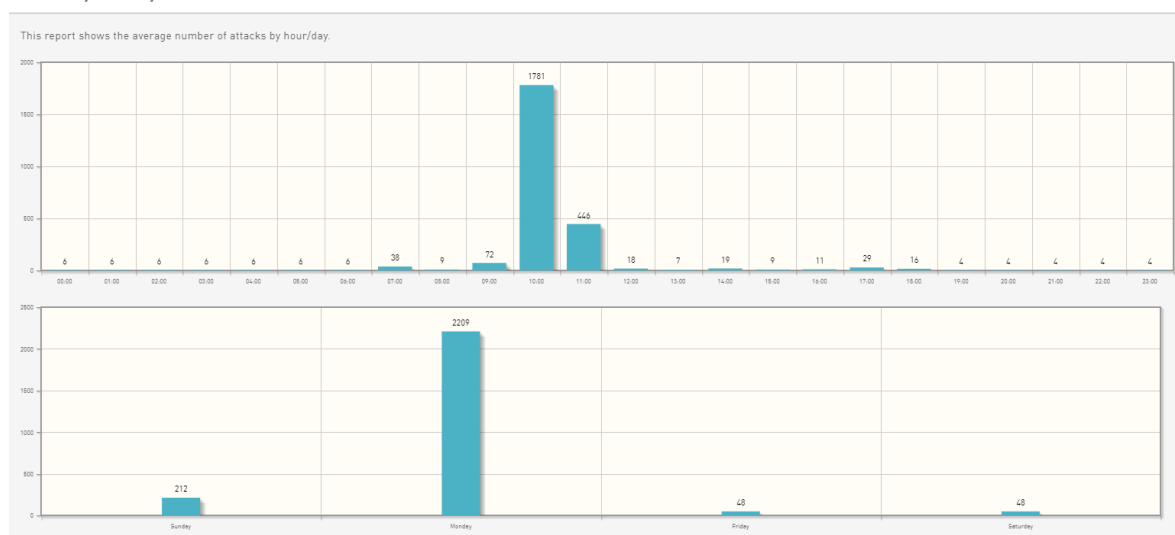
Attacks by Hour/Day

This report shows patterns of attacks occurring within a selected period of time. Data is displayed according to the distribution of attacks during specific hours and days of the week.

An Attacks by Hour/Day report can be presented in either of the following formats:

Graph: Data is presented in bar graph form. Hourly statistics appear on the top, and daily statistics are shown on the bottom. For example:

Attacks by Hour/Day



- **Text:** Data is presented in table form. Daily statistics appear on the top, and hourly statistics are shown on the bottom. For example:

Attacks by Hour/Day

This report shows the average number of attacks by hour/day.

DAY	EVENTS
Sunday	24
Monday	82
Tuesday	2221
Wednesday	1209
Thursday	1674
Friday	27

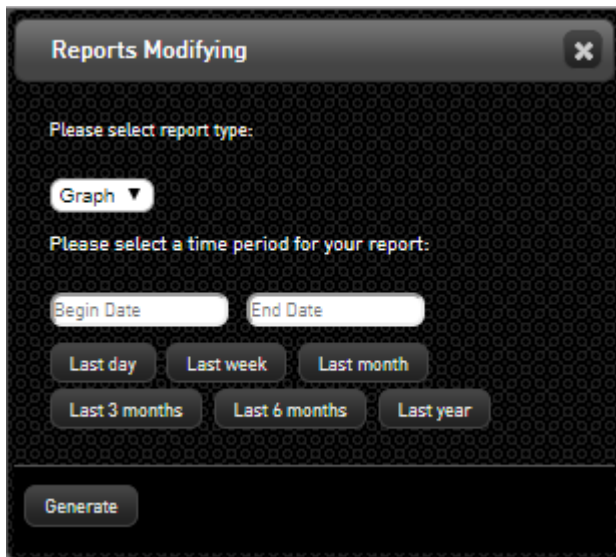
HOUR	EVENTS
00:00	386
01:00	32
02:00	32
07:00	6
08:00	530
09:00	23
10:00	151
11:00	434
12:00	353

Note

Missing hours or days indicate that no attacks occurred during that hour/day.

To generate an Attacks by Hour/Day report:

1. From the left side of the **Reports** tab, select **Attacks by Hour/Day**.
The **Reports Modifying** dialog opens.

A screenshot of a 'Reports Modifying' dialog box. The dialog has a title bar with the text 'Reports Modifying' and a close button (X). Inside, there are two sections. The first section is titled 'Please select report type:' and contains a dropdown menu with 'Graph' selected. The second section is titled 'Please select a time period for your report:' and contains two text input fields labeled 'Begin Date' and 'End Date'. Below these fields are six buttons: 'Last day', 'Last week', 'Last month', 'Last 3 months', 'Last 6 months', and 'Last year'. At the bottom of the dialog is a 'Generate' button.

2. From the dropdown list at the top of the dialog, select the desired display format (**Graph** or **Text**).
3. Select a time period for the report by clicking one of the buttons. Alternatively, specify a custom timeframe by clicking in the **Begin Date** and **End Date** fields and selecting a start and end date on the Calendar popups.
4. Click **Generate**.
The report is displayed.

Prevented Processes

This report lists the file paths of the processes whose activities were most recently prevented by the Detection and Response Agent. The processes, which are differentiated by MD5 identifier, are listed in the order of number of prevention instances.

Prevented Processes	
This report describes the last (up to 100) processes whose activities were prevented.	
PROCESS	PREVENTIONS
C:\ProgramData\ezlfrzgxkislolj399\tasksche.exe	5386
C:\USERS\ADMINISTRATOR\NOBFUDYCOMAL.EXE	1598
C:\Users\ga\Desktop\wannacry.exe	1312
C:\USERS\ADMINISTRATOR\APPDATA\LOCAL\TEMP\YOXPTYWY.EXE	449
C:\Users\Freddy\AppData\Roaming\{848E9C45-243D-03FE-7263-F2366FFA2C19}\msconfig.exe	217
C:\USERS\ADMINISTRATOR\APPDATA\LOCAL\DRPBX\DRPBX.EXE	97
C:\USERS\ADMINISTRATOR\APPDATA\ROAMING\FRFX\FIREFOX.EXE	95
C:\USERS\ADMINISTRATOR\DESKTOP\PT KIT-20160911T073459Z\PT KIT\BART\BART.EXE	90
C:\USERS\ADMINISTRATOR\APPDATA\LOCAL\TEMP\SVCHOST.EXE	69
C:\USERS\ADMINISTRATOR\DESKTOP\PT KIT-20160911T073459Z\PT KIT\CUTWAIL\CUTWAIL.EXE	49
C:\Windows\SysWOW64\rundll32.exe	2
C:\USERS\ADMINISTRATOR\APPDATA\LOCAL\TEMP\C0CF40B8830D666A24BDD4FEBDC162E95AA30ED968FA3675E26AD97B2E88E03A.EXE	2

Detection and Response Monitoring Environment User Activity

This report provides a high level breakdown of user status and activities. The table on the left displays the total number of users assigned to each role. The table on the right lists total instances of user activities (performed by all users), broken down according to type.

Paranoid Management Environment's User Activities			
This report describes status and activity of the PME's users (since the beginning).			
Users by Role		User Activities	
USER ROLE	COUNT	ACTIVITY	COUNT
Roots	6	SERVER	1
Admins	2	Editing users	19
Super Users	0	Login	303
Viewers	1	Logout	49
Total	9	Auto approvement	1
		Licensing server	1
		Packages	17
		Editing endpoints	83
		send	11
		Editing policies	247
		Editing events	355
		Database Actions	16

Managing Users

The **Users** tab allows you to view and manage the users who are authorized to log into the Detection and Response Monitoring Environment. Detection and Response supports the following

types of users:

- **Viewer:** Has read-only privileges in the Detection and Response Monitoring Environment.
- **Admin:** Has privileges to perform all routine activities related to maintenance and management of the environment. The Admin can handle security events (e.g., create/edit and assign Exceptions, solve events), manage endpoints (e.g., assign endpoints to Groups, configure Group settings excluding Advanced Settings) and more.
- **Root:** In addition to all Admin permissions, has privileges to perform more sensitive actions such as creating Hardening Policies, configuring Advanced Settings for Groups (e.g., defining Trusted Applications), performing database management activities and more. In addition, Root users are authorized to access the Detection and Response Management Console.

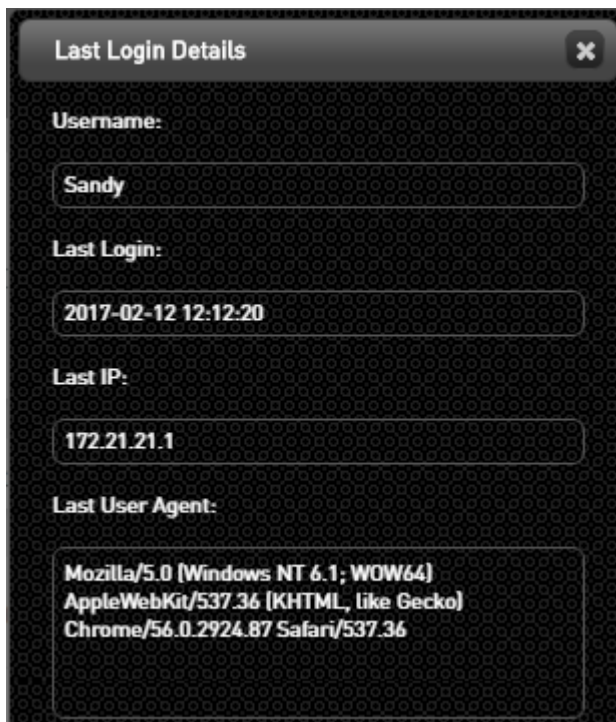
The grid in the **Users** tab displays general information about each user. The columns are described in the table below the figure.

in the table below the figure.

DASHBOARD	ENDPOINTS	USERS	LOGS ▶	POLICIES	GROUPS	PROCESSES
Username	Level	Last Login	Last User Agent	Last IP	Options	
WarRoom	Viewer	2016-12-26 13:42:28		172.21.21.1	Edit User	
adi	Viewer	2016-10-06 13:21:02	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 [KHTML, like Gecko] Chr...	172.21.1.142	Edit User	
nyotronviewer	Viewer	2016-10-21 17:06:29	None	0.0.0.0	Edit User	
Sandy	Admin	2017-03-13 10:32:44	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 [KHTML, like Gecko] Chrome...	172.21.21.1	Edit My User	
tester2	Admin	2017-02-12 17:41:46	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 [KHTML, like Gecko] Chr...	172.21.21.1	Edit User	
Create New User						

Column	Description
Username	Name used to access the Detection and Response Monitoring Environment.
Level	User type (Viewer, Super User, etc.).
Last Login	Date and time of most recent Detection and Response Monitoring Environment login.
Last User Agent	Details about the browser used for the last login.
Last IP	IP address of the machine from which the user last logged in.
Options	Clicking this link opens the Edit User dialog, where you can modify user parameters. For more information, refer to Updating User Details .

Clicking the **Last Login** or **Last User Agent** value in a row in the Users grid opens a popup that displays the information about the selected user in a consolidated, easy to view format.



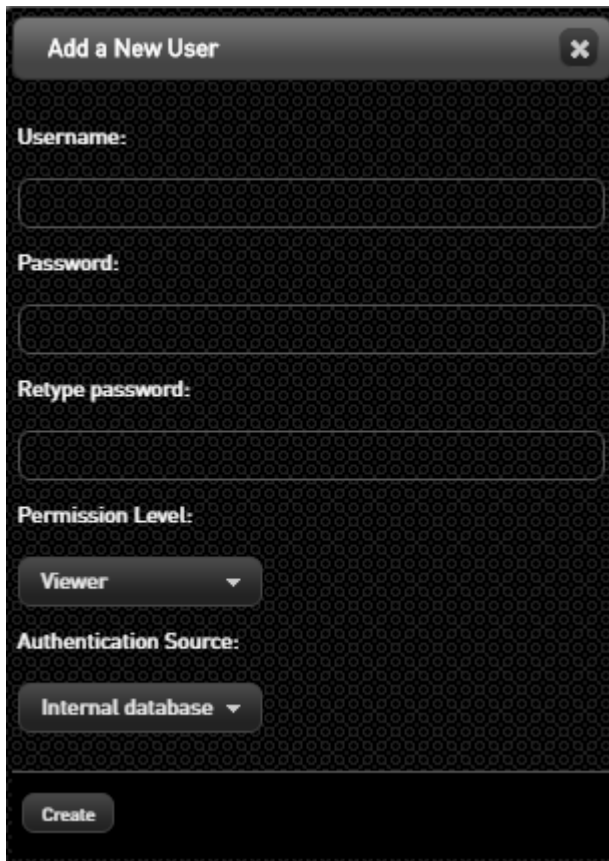
Adding New Users

Creating a new user involves specifying user login credentials and a permissions level for the user. In addition, you need to select an authentication source for user login (internal database or Active Directory). When selecting Active Directory, verify that Active Directory domains have been defined in the **Server Management** menu.

To add a new user to the system:

1. At the lower left corner of the Users tab, click **Create New User**.

The **Add a New User** dialog opens.



Add a New User [X]

Username:

Password:

Retype password:

Permission Level:

Viewer ▼

Authentication Source:

Internal database ▼

Create

2. Define login credentials for the new user by entering a username and password in the appropriate fields. Then, re-enter the password in the **Retype password** field.
3. From the **Permission Level** dropdown list, select the relevant authorization category for the new user.
4. From the **Authentication Source** dropdown list, select the relevant login authentication source.
5. Click **Create**.

The **Add a New User** dialog closes, and the new user is saved in the system.

Updating User Details

The **Edit User** dialog enables you to update one or more details of other users. (For information about modifying your own details, refer to [Updating Your Own User Details](#).)

To update user details:

1. From the **Users** tab, at the right side of the relevant row, click **Edit User**.

The **Edit User** dialog opens.

Edit User [X]

New username:
nyotronviewer

New password:
[Empty field]

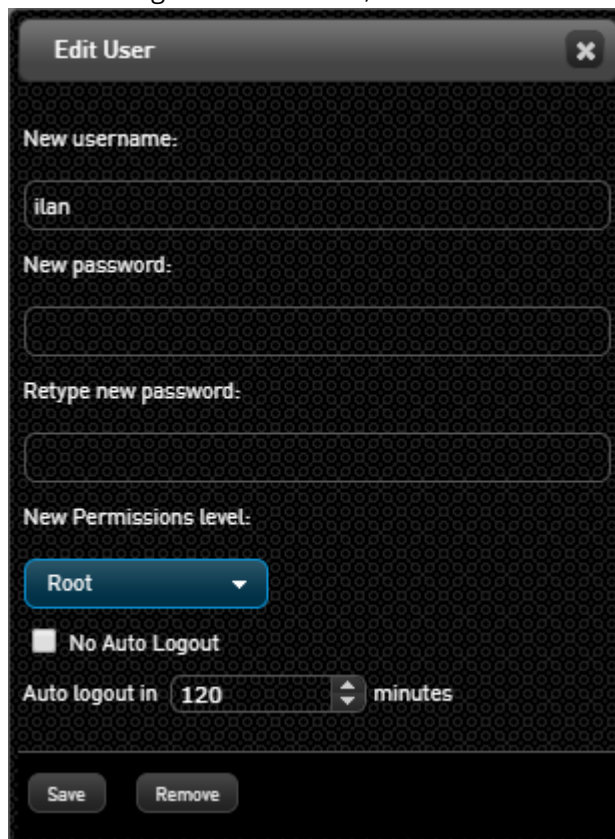
Retype new password:
[Empty field]

New Permissions level:
Viewer ▼

Save

2. Update any of the following details, as required:
 - **Username:** Enter the new name in the **New username** field.
 - **Password:** Enter the password in the **New password** field. Then, re-enter it in the **Retype new password** field.
 - **User type:** Select the relevant permissions level from the **New Permissions level** dropdown list.
 - **Auto Logout value:** Specify the period of time (in minutes) after which the user's Detection and Response Monitoring Environment session will automatically end. If you do not want to

limit the length of the session, select the **No Auto Logout** checkbox.



Edit User

New username:
ilan

New password:

Retype new password:

New Permissions level:
Root

☐ No Auto Logout

Auto logout in 120 minutes

Save Remove

3. Click **Save**.

The **Edit User** dialog closes, and changes are saved in the system.

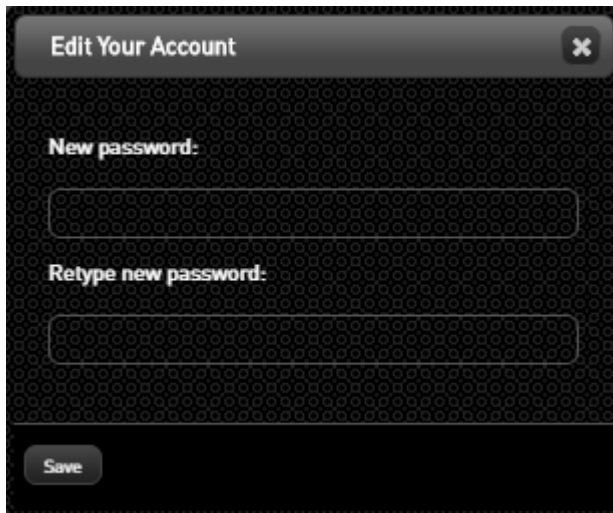
Updating Your Own User Details

Updating the details of your own user account involves password management only. Detection and Response does not allow you to change your own username or permissions level.

To update your own user details:

1. From the **Users** tab, at the right side of the relevant row, click **Edit My User**.

The **Edit Your Account** dialog opens.

The image shows a dark-themed dialog box titled "Edit Your Account" with a close button (X) in the top right corner. Inside the dialog, there are two text input fields. The first is labeled "New password:" and the second is labeled "Retype new password:". At the bottom left of the dialog is a "Save" button.

2. Enter your new password in the **New password** field. Then, re-enter it in the **Retype new password** field.
3. Click **Save**.

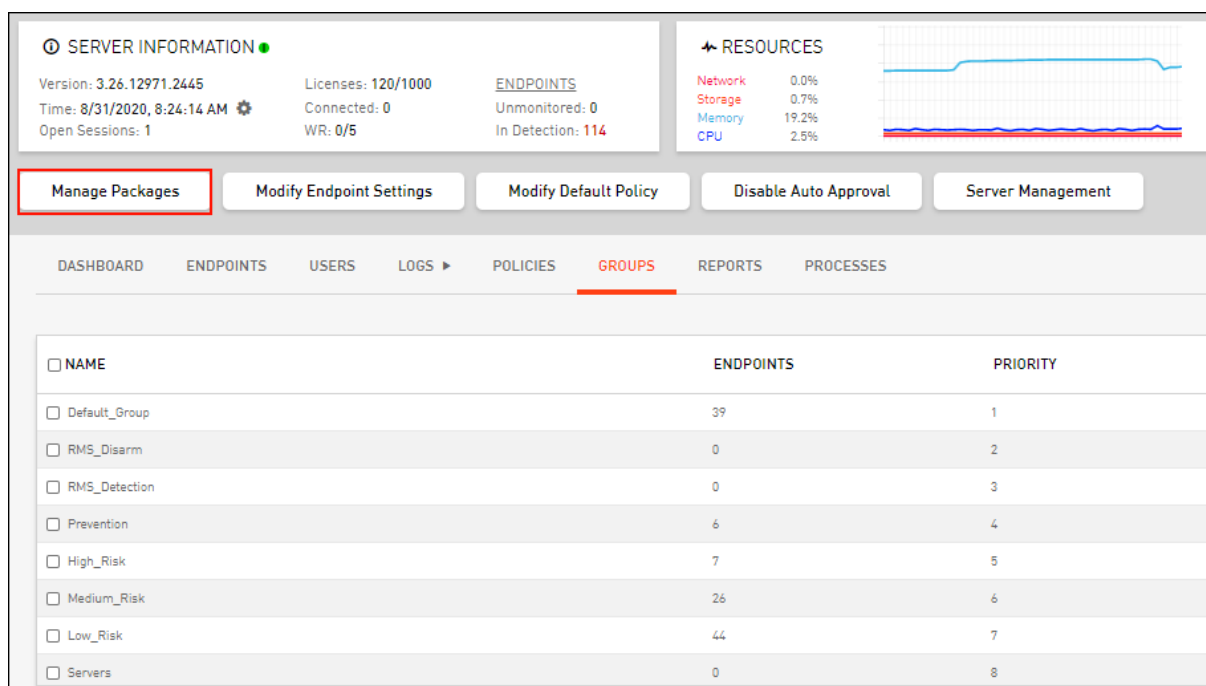
The **Edit Your Account** dialog closes, and your new password is saved in the system.

Handling Update Packages

A package is a compressed file provided by Acronis that contains updates for Detection and Response system components (Agent, BPM, and server). It is recommended to store packages in a dedicated folder for easy access and reference.

The **Manage Packages** button enables you to handle all aspects of package management, including:

- [Uploading packages](#) to the Detection and Response system
- Viewing the current server version
- Viewing and managing lists of [uploaded Agent and BPM versions](#)
- Viewing the most recent log files retrieved from endpoints



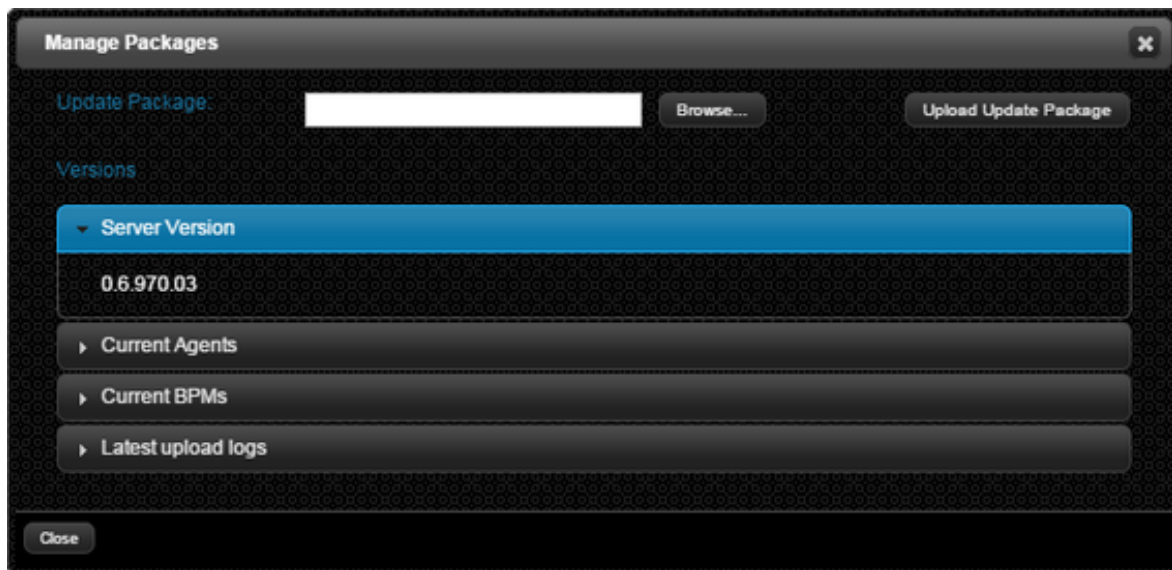
Uploading Update Packages

The Update Package feature allows you to upload a selected package (Server, Agent or BPM) to the system. When a server update package is uploaded, automatic installation of the server upgrade begins immediately. When you upload an Agent or a BPM update package, the new Agent / BPM versions are listed in the [Current Agents and Current BPMs frames](#) of the **Manage Packages** popup. You can then assign these versions as default endpoint settings, or apply them to relevant endpoints Groups.

To upload an update package to the system:

1. At the upper left side of the Detection and Response Monitoring Environment console, click **Manage Packages**.

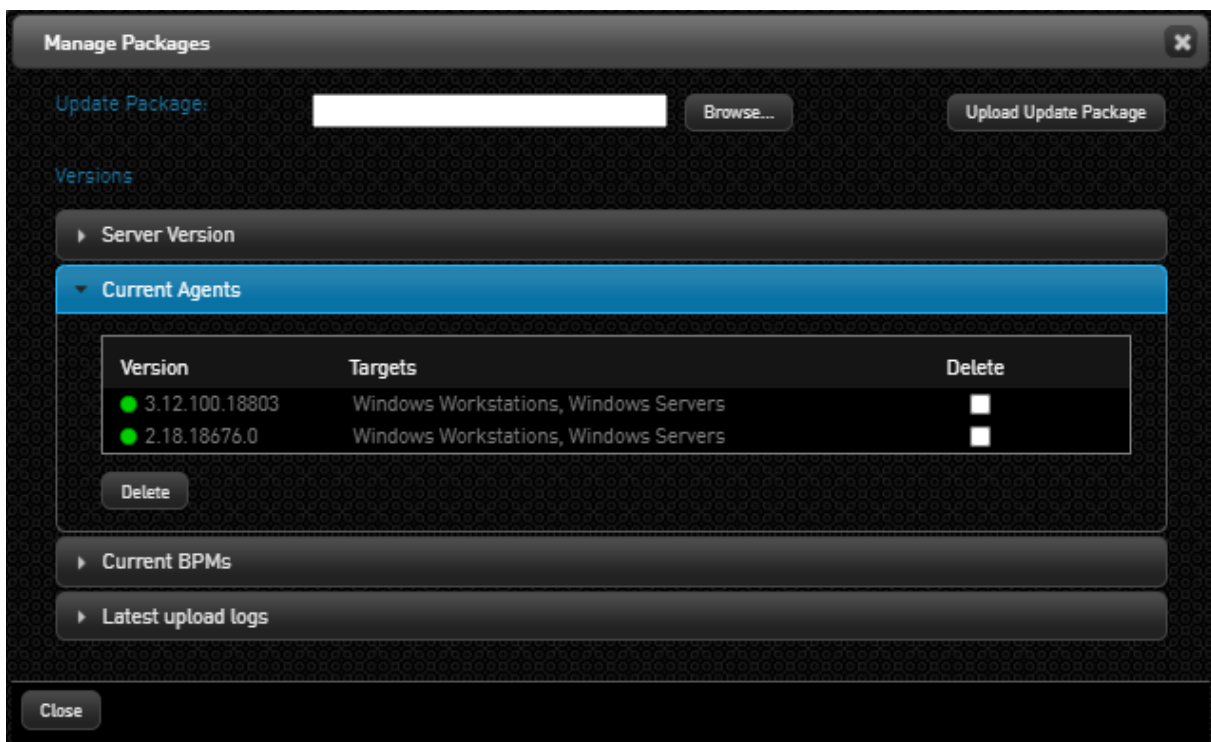
The **Manage Packages** popup opens.



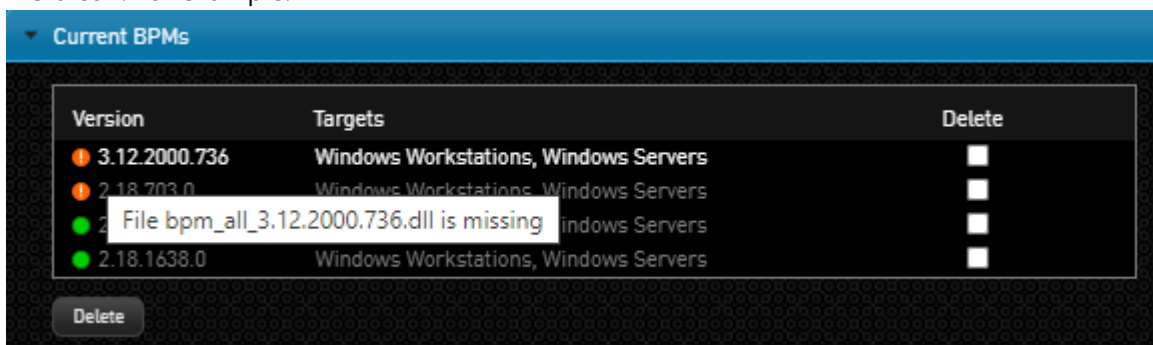
2. At the top of the popup, click **Browse**.
The **Open** dialog is displayed.
3. Navigate to and select the relevant update package. Then, click **Open**.
The **Open** dialog closes, and the path of the selected file appears in the **Update Package** field.
4. Click **Upload Update Package**.
A progress bar is displayed while the package is uploading. When the upload is complete, a confirmation message appears.

Managing Agent and BPM Versions

Detection and Response maintains an inventory of all Agent and BPM versions that have been previously uploaded. The **Current Agents** and **Current BPMs** frames display lists of the uploaded versions and the types of machines to which these versions can be deployed (Workstations and/or Servers). The Delete function enables you to remove versions that are no longer required.



To help ensure a successful update process, each version has a colored indicator icon to its left. Green icons (as in the example above) indicate that there are no current issues with the file. Files that are registered in the database but are not actually in the file system are indicated by an orange Alert icon. For example:



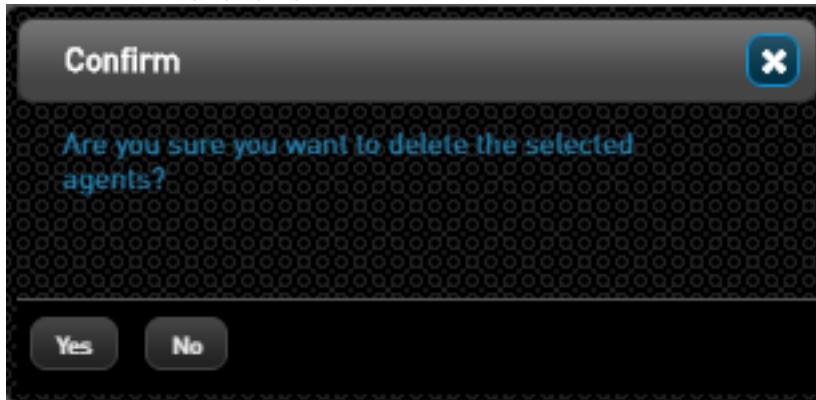
The following procedure explains how to delete unnecessary Agent versions. The same procedure can be used in the **Current BPMs** frame to delete unused BPM versions.

To delete Agent versions from the system:

1. At the upper left side of the Detection and Response Monitoring Environment console, click **Manage Packages**.
The **Manage Packages** popup opens.
2. Open the **Current Agents** frame by selecting **Current Agents**.
3. At the right side of the frame, select the checkboxes in the rows of the Agent versions that you want to remove.

Click **Delete**.

A confirmation popup opens.



4.

5. Click **Yes**.

All the popups close, and the selected versions are deleted from the system.

Defining License Approval Settings

As part of the Agent installation process, the Detection and Response Server needs to approve the Agent's connection and license consumption. To enable this approval, the server must be configured to handle license distribution.

Once the Detection and Response Server has been designated as a licensing server, you can configure the license approval process to be automatic (by the server) or manual (by an administrator).

Note

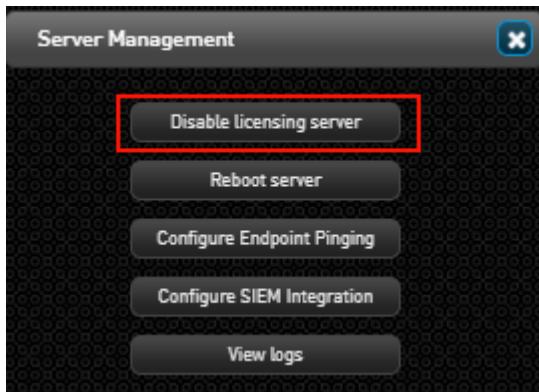
Disabling or enabling the server from handling license distribution affects new Detection and Response Agents only. Agents that were connected prior to changing the licensing setting continue to report to the server.

To configure license approval settings:

1. At the top of the Detection and Response Monitoring Environment console, click **Server Management**.

The **Server Management** popup opens.

2. At the top of the popup, verify that the button label is **Disable licensing server**. (This indicates that the server is configured to handle license distribution.)

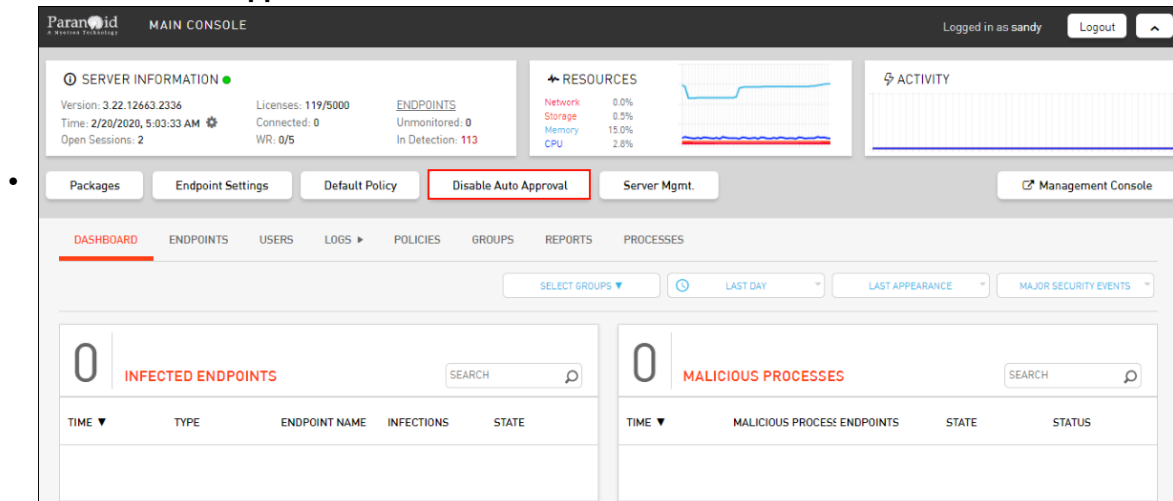


If the button label is **Enable licensing server**, click it to enable the server to handle licensing.

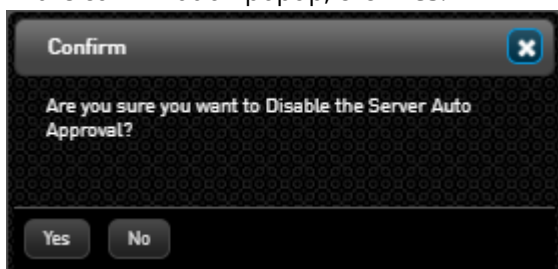
- At the top of the Detection and Response Monitoring Environment console, toggle the **Auto Approval** button to set the required approval configuration:

- To support automatic license approval by the server, verify that the button label is **Disable Auto Approval**.

To block automatic license approval and support manual approval, verify that the button label is **Enable Auto Approval**.



In the confirmation popup, click **Yes**.



4.

Viewing User Records in the Logs Tab

Detection and Response automatically records each action performed by every user, and maintains these records in log files. The **Logs** tab provides a high level summary of these actions.

The main features of the tab are described in the table below the diagram.

DASHBOARD

ENDPOINTS

USERS

LOGS ▶1

POLICIES

GROUPS

REPORTS

PROCESSES

2

DATE:

YYYY-MM-DD

 /

YYYY-MM-DD

ALL USERS ×

ALL CATEGORIES

FILTER

TIME ▼	USERNAME	ACTION	CATEGORY
2019-11-25 07:29:51	SANDY	LOGGED IN FROM IP: 84.94.217.218	LOGIN
2019-11-25 07:22:58	SANDY	DISCONNECTED FROM IP: 84.94.217.218	LOGOUT
2019-11-25 06:26:34	SANDY	WARNING: NUMBER OF ASSIGNED DEFAULT EXCEPTIONS HAS EXCEEDED	SERVERLOGS
2019-11-25 05:54:53	SANDY	LOGGED IN FROM IP: 84.94.217.218	LOGIN
2019-11-25 04:45:44	SANDY	DISCONNECTED FROM IP: 84.94.217.218	LOGOUT

Delete Logs

5

<<

<

1 / 2112

>

>>

Number	Feature	Description
1	Mode selector	Click this icon to toggle between Auto Refresh mode (in which the log records are continuously updated) and Pause mode (in which you need to manually refresh the list). During Pause mode, the icon appears as follows: <div>LOGS </div>
2	Filters	Provide a variety of filtering options to help you quickly find specific information. For details, refer to Filtering the Log Records .
3	Logs grid	Lists basic information about each action. You can sort the grid according to any column. Clicking any row opens a popup displaying the data in an easy to read format.
4	Delete button	Allows authorized users to remove log records that are no longer relevant. For details, refer to Deleting Log Records .
5	Navigation bar	Allows you to quickly navigate to the first, previous, next or last page of a multi-page Logs record.

Filtering the Log Records

The filtering options above the Logs grid enable you to search for an action or set of actions according to a variety of criteria. The filtering options can be combined to define very specific search criteria, as required.

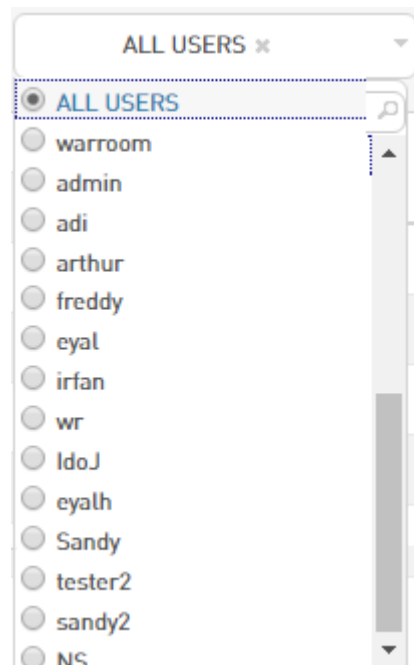
DASHBOARD	ENDPOINTS	USERS	LOGS ▶	POLICIES	GROUPS	REPORTS	PROCESSES
<div> <div>DATE: <input type="text" value="YYYY-MM-DD"/> / <input type="text" value="YYYY-MM-DD"/></div> <div>ALL USERS <input type="text" value="x"/></div> <div>ALL CATEGORIES</div> <div>FILTER</div> </div>							
TIME ▼	USERNAME	ACTION					
2019-11-25 07:29:51	SANDY	LOGGED IN FROM IP: 84.94.217.218					
2019-11-25 07:22:58	SANDY	DISCONNECTED FROM IP: 84.94.217.218					
2019-11-25 06:26:34	SANDY	WARNING: NUMBER OF ASSIGNED DEFAULT EXCEPTIONS HAS EXCEEDED					
2019-11-25 05:54:53	SANDY	LOGGED IN FROM IP: 84.94.217.218					
2019-11-25 04:45:44	SANDY	DISCONNECTED FROM IP: 84.94.217.218					

The options are:

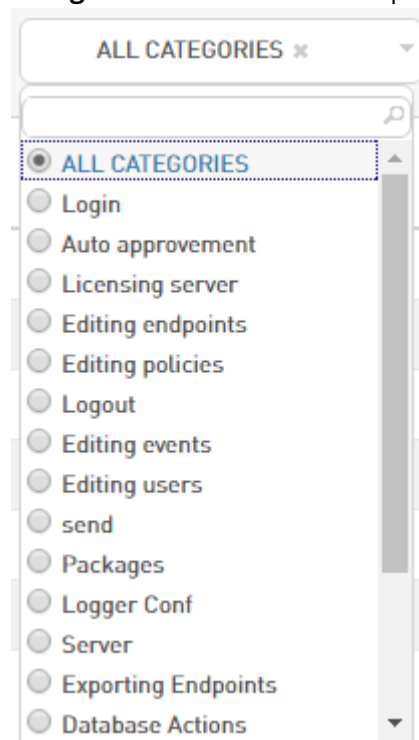
Date filter: Filters for actions that occurred within a specified timeframe. Click the date fields to open the date picker, and select the relevant start and end dates.



Users filter: Filters for actions of a specified user.



Categories filter: Filters for a specific category of actions.



To filter the log records:

1. At the top of the **Logs** tab, specify the required search timeframe, and/or select the relevant user and/or category from the lists. (Only one user and category may be selected.)
2. Click **FILTER**.
The **CLEAR** button appears next to the **FILTER** button, and the list of records is filtered according to the selected criteria.
3. To clear filtering and display the complete log records, click **CLEAR**.

Deleting Log Records

The list of user actions displayed in the **Logs** tab of the Detection and Response Monitoring Environment can quickly become lengthy and unmanageable. The Delete Logs action allows authorized users to remove log records that are no longer relevant.

DASHBOARD

ENDPOINTS

USERS

LOGS ▶

POLICIES

GROUPS

REPORTS

PROCESSES

DATE: /

TIME ▼	USERNAME	ACTION
2019-11-25 07:29:51	SANDY	LOGGED IN FROM IP: 84.94.217.218
2019-11-25 07:22:58	SANDY	DISCONNECTED FROM IP: 84.94.217.218
2019-11-25 06:26:34	SANDY	WARNING: NUMBER OF ASSIGNED DEFAULT EXCEPTIONS HAS EXCEEDED
2019-11-25 05:54:53	SANDY	LOGGED IN FROM IP: 84.94.217.218
2019-11-25 04:45:44	SANDY	DISCONNECTED FROM IP: 84.94.217.218

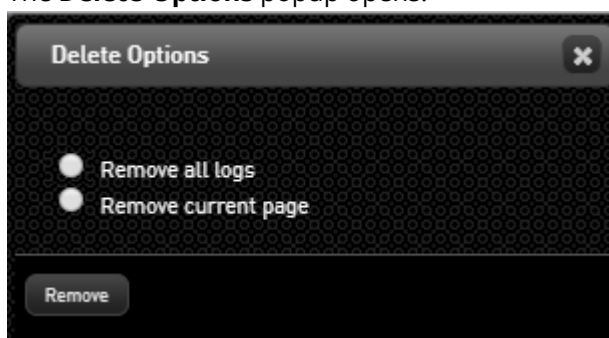
Delete Logs

When removing log records, you can choose to delete the entire list, or remove only the entries listed on the current page of the list.

To delete log records:

At the lower left corner of the **Logs** tab, click **Delete Logs**.

The **Delete Options** popup opens.



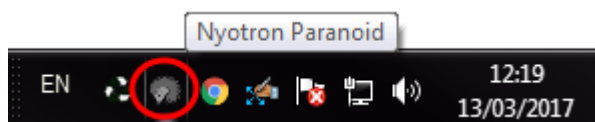
- 1.
2. Select the relevant radio button, and then click **Remove**.

The selected log records are deleted from the list.

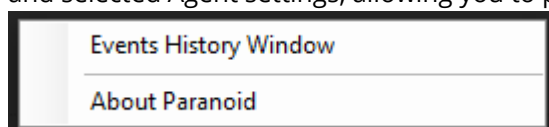
Managing Detection and Response from an Endpoint

When the Detection and Response Agent is deployed on an endpoint where the [Icon setting](#) is

enabled, the Detection and Response icon  appears in the endpoint's system tray.



Clicking the Detection and Response icon opens a list of options that let you review detected events and selected Agent settings, allowing you to perform local endpoint analysis.



Viewing Events History

Selecting the Events History Window option opens the **Acronis Detection and Response Events History** window. This window displays a list of events that the Detection and Response Agent detected or prevented on the endpoint.

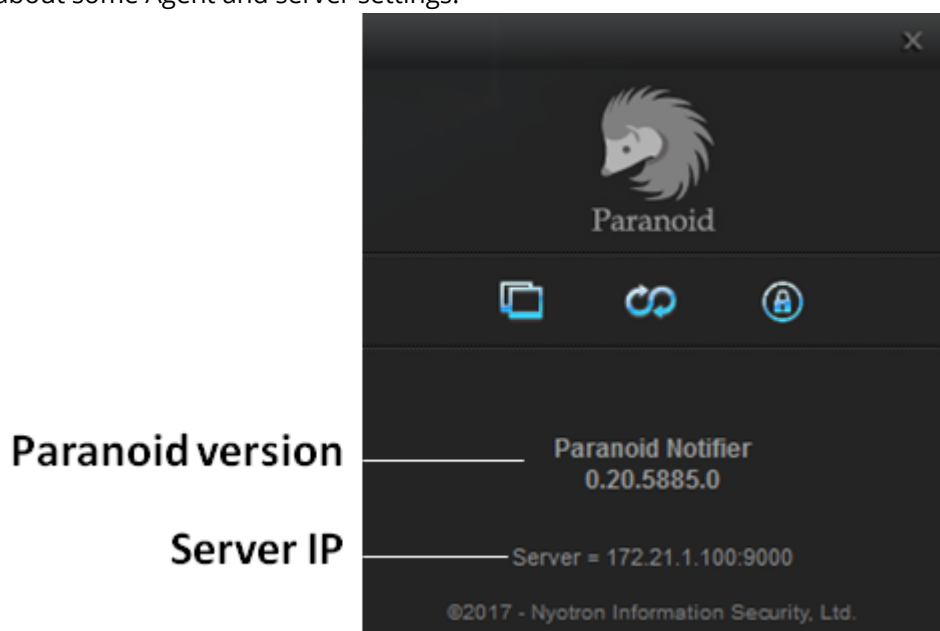
Nyotron Paranoid Events History							
#	Date & Time	Id	Priority	N...	Slot	Event	Path
14	4/2/2017 11:58:20 AM	2221	3.100	49	OSP	ARBITRARY_CODE_ACTIVITY	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
13	4/2/2017 11:58:09 AM	2221	3.100	49	OSP	ARBITRARY_CODE_ACTIVITY	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
12	4/2/2017 11:58:09 AM	2221	3.100	49	OSP	ARBITRARY_CODE_ACTIVITY	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
11	4/2/2017 11:58:09 AM	2221	3.100	49	OSP	ARBITRARY_CODE_ACTIVITY	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
10	4/2/2017 11:58:03 AM	2221	3.100	49	OSP	ARBITRARY_CODE_ACTIVITY	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
9	4/2/2017 11:58:03 AM	1502	3.100	50	OSP	ARBITRARY_CODE_EXECUTION	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
8	4/2/2017 11:58:03 AM	1510	3.100	247	OSP	AUTORUN_SETTINGS	(REGISTRY\USER\S-1-5-21-1155161494-921974304-11477885
7	4/2/2017 11:58:03 AM	1502	3.100	50	OSP	ARBITRARY_CODE_EXECUTION	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
6	4/2/2017 11:58:03 AM	1502	3.100	50	OSP	ARBITRARY_CODE_EXECUTION	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
4	4/2/2017 11:58:03 AM	1502	3.100	50	OSP	ARBITRARY_CODE_EXECUTION	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
3	4/2/2017 11:58:02 AM	1502	3.100	50	OSP	ARBITRARY_CODE_EXECUTION	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
5	4/2/2017 11:58:02 AM	1502	3.100	50	OSP	ARBITRARY_CODE_EXECUTION	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
2	4/2/2017 11:58:01 AM	2221	3.100	49	OSP	ARBITRARY_CODE_ACTIVITY	C:\WINDOWS\SYSWOW64\EXPLORER.EXE
1	4/2/2017 11:58:01 AM	2226	3.100	50	OSP	ARBITRARY_CODE_EXECUTION	C:\USERS\QA\APPDATA\ROAMING\DUFY\ORHA\EXE C:\WINDOWS\SYSWOW64\EXPLORER.EXE

Important information provided by the **Acronis Detection and Response Events History** window includes:




- **Date & Time:** Timestamp of when the event was detected/prevented.
- **Event:** The Protection Module impacted by the event.
- **Program:** The process that triggered the event.

Viewing Selected Detection and Response Settings

Selecting the About Detection and Response option opens a window that shows you information about some Agent and server settings.



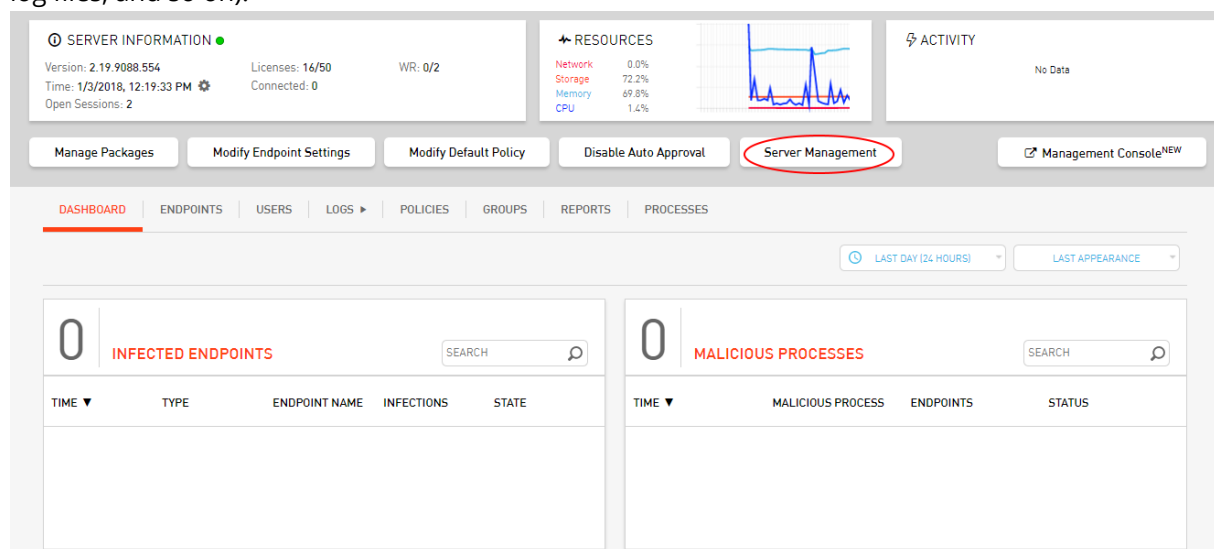
The icons below the Detection and Response logo indicate Agent mode, notification setting and connection status:

Icon	Description
	Indicates current setting for popup notifications. When popups are enabled, the icon is blue. When popups are disabled, the icon is gray.
	Shows current server connection status. A connection issue is indicated by a gray icon.
	Indicate current Agent mode. In Prevention mode, the icon is blue. In Detection mode, the icon is gray.

Performing Server Administration

Server Management Operations

The **Server Management** button opens a popup from which you can perform various actions related to server configuration and operation (e.g., starting and stopping the server, working with log files, and so on).



Available actions are listed in the table below.

Action	Description
Disable/Enable licensing server	Controls the ability of the server to handle license distribution for new Agents. For more information, refer to Defining License Approval Settings .
Reboot server	Starts the Detection and Response server after a shutdown.
Configure Endpoint Ping	Controls the ability to ping endpoints, for more effective troubleshooting of offline endpoints. For details, refer to Configuring Endpoint Pinging Capability .
Configure SIEM Integration	Displays the configuration settings necessary for server data to be utilized by SIEM products and services. For more information, refer to Configuring SIEM Integration .
Configure SAML Integration	Displays the configuration settings for integration with SAML. For more information, refer to Configuring SAML Integration .
View logs	Allows you to view and download any log file generated by the server. For more information, refer to Viewing and Downloading Log Files .
Agent Offline Installation	Enables you to create customized packages for local installation of the Agent on new endpoints or for local upgrade of Agents on existing endpoints. For details, refer to Handling Agent Offline Installation .
Configure bandwidth	Allows you to define settings for throttled data transfer. For details, refer to Controlling Network Usage .

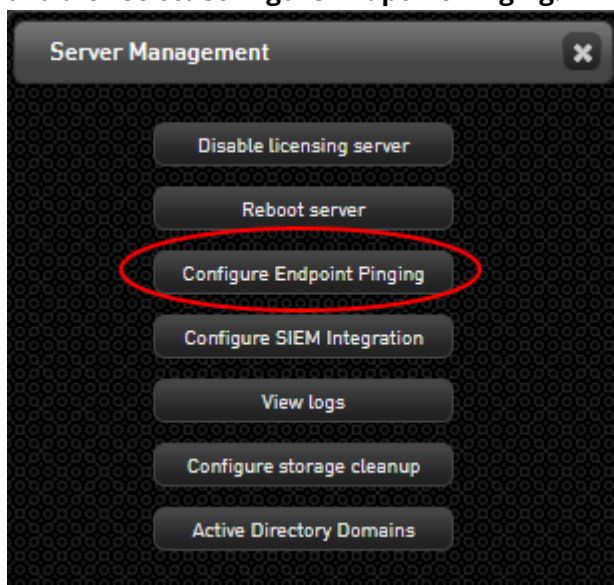
Action	Description
Storage Management	Enables you to define settings for storage alert messages and perform cleanup actions to create more storage space. For details, refer to Managing Server Storage .
Active Directory Domains	Enables you to define Active Directory integration settings.
Database Management	Allows you to management database files and perform database operations. For more information, refer to Handling Database Files .
Reset pending operations	Resets background server operations (relevant for server upgrade troubleshooting).

Configuring Endpoint Pinging Capability

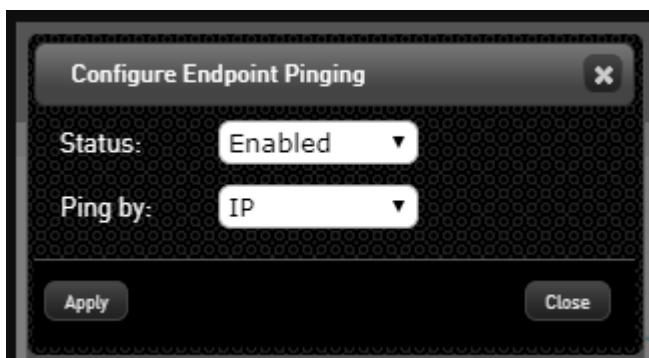
Detection and Response supports the ability to ping endpoints, so you can troubleshoot offline endpoints effectively. The Configure Endpoint Pinging feature lets you enable and disable endpoint pinging capability. When pinging is enabled, you can set pinging to either IP or hostname.

To configure endpoint pinging:

From the Detection and Response Monitoring Environment console, click **Server Management**, and then select **Configure Endpoint Pinging**.



1. The **Configure Endpoint Pinging** dialog opens.



2. Activate or disable endpoint ping by selecting **Enabled** or **Disabled** from the **Status** dropdown.
3. When ping is enabled, specify the ping method by selecting **IP** or **Hostname** from the **Ping by** dropdown.
4. Click **Apply**.
Changes are saved in the system.

Configuring SIEM Integration

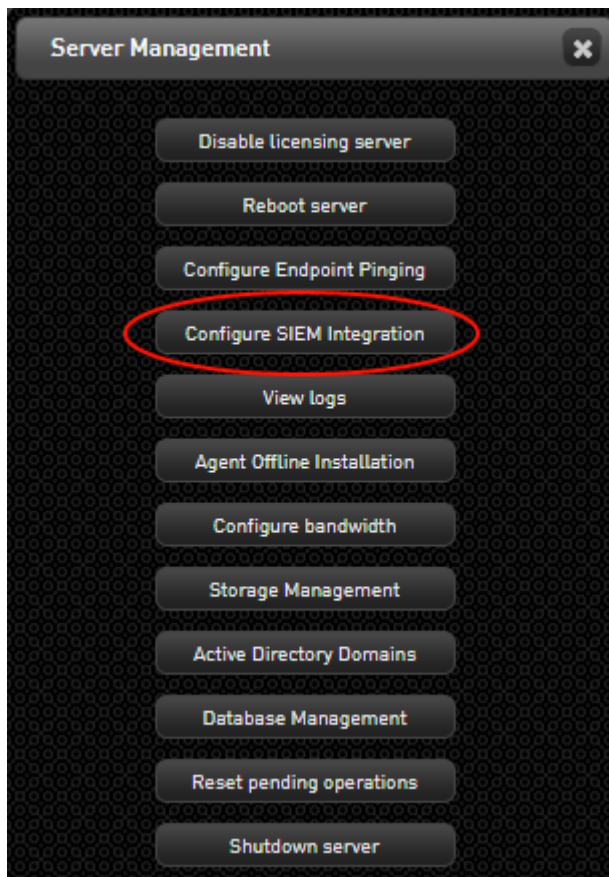
With SIEM integration, the Detection and Response solution is seamlessly incorporated into a customer's existing security infrastructure. Security Operations Center (SOC) analysts are thus able to monitor Detection and Response alerts from their familiar native SIEM systems. Detection and Response is able to integrate with SIEM systems through either Syslog or CEF (Common Event Format) log formats.

Specifying SIEM Integration Settings

The Configure SIEM Integration action involves defining or updating the configuration settings necessary for Detection and Response Server data to be utilized by external SIEM services. The settings you define should be provided or recommended by the SIEM solution that you work with.

To define or update SIEM integration settings:

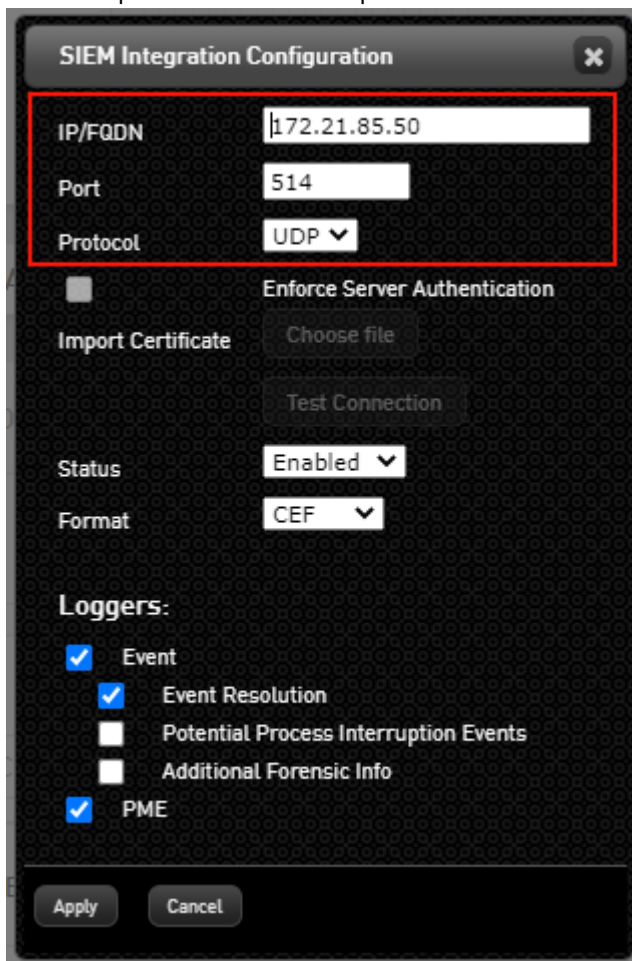
1. At the top of the Detection and Response Monitoring Environment console, select **Server Management > Configure SIEM Integration**.



The **SIEM Integration Configuration** popup opens.

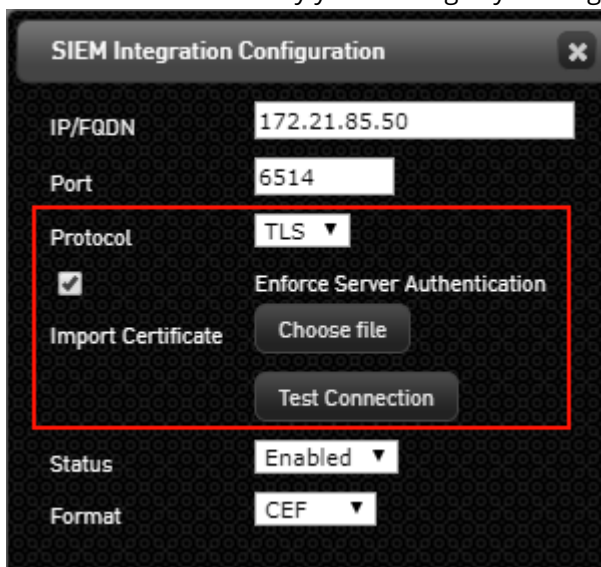
2. From the **Protocol** dropdown, choose the desired protocol (**UDP** or **TLS**). Then, enter the relevant IP and port in the appropriate fields.

The UDP port is **514**. The TLS port is **6514**.



The image shows a 'SIEM Integration Configuration' dialog box. A red rectangle highlights the top section containing the following fields: 'IP/FQDN' with the value '172.21.85.50', 'Port' with the value '514', and 'Protocol' with a dropdown menu set to 'UDP'. Below this, there is an unchecked checkbox for 'Enforce Server Authentication', an 'Import Certificate' section with a 'Choose file' button, and a 'Test Connection' button. Further down, the 'Status' is set to 'Enabled' and the 'Format' is set to 'CEF'. A 'Loggers' section contains five items: 'Event' (checked), 'Event Resolution' (checked), 'Potential Process Interruption Events' (unchecked), 'Additional Forensic Info' (unchecked), and 'PME' (checked). At the bottom are 'Apply' and 'Cancel' buttons.

If you selected the TLS protocol and you want to enforce server authentication before communication is allowed, select the checkbox, click **Choose file** and navigate to the relevant certificate. You can verify your settings by clicking **Test Connection**.



The image shows the same 'SIEM Integration Configuration' dialog box, but with different settings. A red rectangle highlights the 'Protocol' dropdown set to 'TLS', the 'Enforce Server Authentication' checkbox which is now checked, the 'Import Certificate' section with the 'Choose file' button, and the 'Test Connection' button. The 'IP/FQDN' remains '172.21.85.50', the 'Port' is now '6514', 'Status' is 'Enabled', and 'Format' is 'CEF'. The 'Loggers' section remains unchanged.

- 3.
4. From the **Status** dropdown list, select **Enabled** or **Disabled**.

Generally the status should be **Enabled**, unless recommended otherwise by your SIEM organization.

5. From the **Format** dropdown list, select **CEF** or **Syslog**.
6. In the **Loggers** section, select or clear the checkboxes, as required. A selected checkbox indicates that the relevant logger is available to the SIEM service.

The following loggers are available:

- **Event:** Contains data about security incidents that are listed as Major Security Events in the Dashboard.

The following additional event-related loggers are available when the **Event** logger is selected:

- **Event Resolution:** Lists security incidents that have been solved or deleted through administrative actions in the Detection and Response Monitoring Environment.
- **Potential Process Interruption Events:** Lists security incidents that were prevented, automatically solved and whitelisted by the Server through creation of an internal Exception.

This logger is not displayed by default. Please contact Acronis Support for more information.

- **Additional Forensic Info:** Includes data about all security incidents (according to the All Security Events filter in the Dashboard.).

This logger is not displayed by default. Please contact Acronis Support for more information.

- **Detection and Response Monitoring Environment:** Contains data about administrative actions taken in the Detection and Response Monitoring Environment, such as changes in Exceptions, Groups, Agent/BPM versions and more.

7. Click **Apply**.

The popup closes, and your updates are saved in the system.

Understanding Events Log Information

The table below lists the fields contained in a CEF Events log. The presence and/or value of some of these fields can vary, depending on the configuration of your environment and the loggers that you make available to the SIEM service.

An example of a field value for each logger type is shown in the last 4 columns of the table. The word *same* indicates that the value would be the same as the Event logger example.

Field Name	Description / Notes	Event example	Additional Forensic Info	Potential Process Interruption	Event Resolution
Prefix1	CEF format version	CEF:0	same	same	same
Prefix2	Device vendor	Acronis	same	same	same

Field Name	Description / Notes	Event example	Additional Forensic Info	Potential Process Interruption	Event Resolution
Prefix3	Device product	Detection and Response	same	same	same
Prefix4	Device version	3.16.11277.1618	same	same	same
Prefix5	Signature ID (indicates the log type)	Events	same	same	same
Prefix6	Event's Protection Module / category	DATA_CORRUPTION	same	same	same
Prefix7	Event's priority	3;4;5	same	7	7
cs1Label	cs1 field description	Endpoint's Agent Version	same	same	N/A
cs1	Endpoint's Agent version	2.18.11816.0	same	same	N/A
cs2Label	cs2 field description	Endpoint's BPM Version	same	same	N/A
cs2	Endpoint's BPM version	2.18.592.0	same	same	N/A
externalId	Event ID (used for drill down in the Detection and Response Monitoring Environment)	16815673	same	same	same
act	Action taken	Prevented; Warning; Detected	same	Prevented - Automatically Whitelist	Solved; Deleted

Field Name	Description / Notes	Event example	Additional Forensic Info	Potential Process Interruption	Event Resolution
				ed	
cs3Label	cs3 field description	Event Type	same	same	N/A
cs3	Event type	File Deletion	same	same	N/A
msg	Short description of event	Sensitive data corruption attempt	same	same	N/A
dvc	Detection and Response Server IP address	127.0.0.1	same	same	N/A
shost	Source hostname	W10-PRD01	same	same	N/A
suser	Source username	john	same	same	N/A
src	Source host address	26.75.120.157	same	same	N/A
dst	Destination host address (relevant for ABNORMAL_COMMUNICATION events only)	103.69.123.252	same	same	N/A
dpt	Destination port (relevant for ABNORMAL_COMMUNICATION events only)	8080	same	same	N/A
filePath	Caller file path	C:\\Windows\\System32\\Malware.exe	same	same	N/A
fileHash	Caller MD5	4e42ee99089042704361cdff7e2057dd	same	same	N/A

Field Name	Description / Notes	Event example	Additional Forensic Info	Potential Process Interruption	Event Resolution
dproc	Callee file path (not relevant for ABNORMAL_COMMUNICATION events)	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe	same	same	N/A
fsize	Caller file size (in bytes)	430592	same	same	N/A
cs4Label	cs4 field description	Command Line	same	same	N/A
cs4	Caller command line	nslookup google.com	same	same	N/A
cs5Label	cs5 field description	Malware Status	same	same	N/A
cs5	Caller external reputation (malware status)	Malware; Not a Malware	same	same	N/A
cs6Label	cs6 field description	callerPublisher	same	same	N/A
cs6	Company or organization that digitally signed the caller process	Microsoft Windows	same	same	N/A
cs7Label	cs7 field description	parentName	same	same	N/A
cs7	Path of the parent process	C:\\Windows\\System32\\cmd.exe	same	same	N/A
cs8Label	cs8 field description	parentPublisher	same	same	N/A

Field Name	Description / Notes	Event example	Additional Forensic Info	Potential Process Interruption	Event Resolution
cs8	Company or organization that digitally signed the parent process	Microsoft Windows	same	same	N/A
cs9Label	cs9 field description	parentMD5	same	same	N/A
cs9	MD5 identifier of the parent	F4F684066175B77E0C3A000549D2922C	same	same	N/A
cs10Label	cs10 field description	Detail Level	same	same	N/A
cs10	Level of detail contained in the log	Major Forensic Info	Additional Forensic Info	Major Forensic Info	N/A
cs11Label**	cs11 field description	OS Type	same	same	N/A
cs11	Operating system(s) of affected machines	Win10	same	same	N/A

** The cs11 field is not displayed by default. Please contact Acronis Support for more information.

The following example shows the syntax of an entry in an Events Log with Additional Forensic Info and OS Type:

```
CEF:0|Acronis|Detection and Response|3.24.12701.2360|Events|ABNORMAL_NETWORK_ACTIVITY|5|cs1Label=Agent Version cs1=3.12.100.18479 cs2Label=BPM Version cs2=3.12.2000.1518 externalId=21096163 act=Prevented msg=Abnormal Network activity attempt. dvc=172.21.2.39 shost=John-PC suser=Administrator src=172.21.2.22 dst=172.21.1.65 dpt=53 filePath=C:\\Windows\\System32\\nslookup.exe fileHash=873B6A4568378AE00123DB99B8AB3857 dproc= fsize=86528 cs4Label=Command Line cs4=nslookup google.com cs5Label=Malware Status cs5=Not a Malware cs6Label=callerPublisher cs6=Microsoft Windows cs7Label=parentName cs7=C:\\Windows\\System32\\cmd.exe cs8Label=parentPublisher cs8=Microsoft Windows cs9Label=parentMD5 cs9=D7AB69FAD18D4A643D84A271DFC0DBDF cs10Label=Detail Level cs10=Additional Forensic Info cs11Label=OS Type cs11=Win10
```

The following example shows the syntax of an entry for a Potential Process Interruption event:

```
CEF:0|Acronis|Detection and Response|3.24.12701.2360|Events|ABNORMAL_NETWORK_
ACTIVITY|7|cs1Label=Agent Version cs1=3.12.100.18479 cs2Label=BPM Version cs2=3.12.2000.1518
externalId=21096163 act=Prevented - Automatically Whitelisted msg=Abnormal Network activity
attempt. dvc=172.21.2.39 shost=John-PC suser=Administrator src=172.21.2.22 dst=172.21.1.65
dpt=53 filePath=C:\\Windows\\System32\\nslookup.exe
fileHash=873B6A4568378AE00123DB99B8AB3857 dproc= fsize=86528 cs4Label=Command Line
cs4=nslookup google.com cs5Label=Malware Status cs5=Not a Malware cs6Label=callerPublisher
cs6=Microsoft Windows cs7Label=parentName cs7=C:\\Windows\\System32\\cmd.exe
cs8Label=parentPublisher cs8=Microsoft Windows cs9Label=parentMD5
cs9=D7AB69FAD18D4A643D84A271DFC0DBDF cs10Label=Detail Level cs10=Major Forensic Info
```

The following example shows the syntax of an entry for an Event Resolution event:

```
CEF:0|Acronis|Detection and Response|3.24.12701.2360|Events|DATA_
CORRUPTION|7|externalId=15447 act=Solved
```

Understanding the Identified Threats Report

The Identified Threats reports is a weekly report listing all detected processes that are recognized as malware but have not yet generated any suspicious activity in your environment (dormant processes). Since these processes produced no security incidents, they will NOT appear in the Detection and Response Management Console Dashboard or in the Detection and Response Management Console Security Center. The Identified Threats reports is designed to raise awareness and help you manage potential security threats in your organization.

The table below lists the fields contained in an Identified Threats report.

Field Name	Description / Notes	Example
Prefix1	CEF format version	CEF:0
Prefix2	Device vendor	Acronis
Prefix3	Device product	Detection and Response
Prefix4	Device version	3.22.12723.2336
Prefix5	Signature ID (indicates the log)	Events

Field Name	Description / Notes	Example
	type)	
Prefix6	Event's Protection Module / category	IDENTIFIED THREAT
Prefix7	Event's priority	5
act	Action taken	Identified
filePath	Caller file path	C:\Users\SOLDCW223\AppData\Roaming\ShopAtHome\ShopAtHomeHelper\ShopAtHomeWatcher.exe
fileHash	Caller MD5	764FAEB61B0645882EE394ABAD4817EA
cs5Label	cs5 field description	Malware Status
cs5	Reputation in VirusTotal	Malware
cs6Label	cs6 field description	Last Appearance
cs6	Date on which the process was most recently detected	2020-01-26 16:33:00
msg	Short description of the event	The process is considered malware and was identified in the environment over the last week

The following example shows the syntax of an entry in an Identified Threats report:

```
Feb 24 06:42:33 host CEF:0|Acronis|Paranoid|3.22.12723.2336|Events|IDENTIFIED THREAT|5|
act=Identified filePath=C:\4e0b892b-bf55-4a5d-b9e2-54ecd3ca5f6c.exe
fileHash=777E57F813C6CD5E85C20DD1FCE25B18 cs5Label=Malware Status cs5=Malware
```

cs6Label="Last Appearance" cs6=2020-02-22 23:30:00 msg=The process is considered malware and was identified in the environment over the last week

Understanding Detection and Response Monitoring Environment Log Information

The table below lists the fields contained in a CEF Detection and Response Monitoring Environment log.

Field Name	Description / Notes	Example
Prefix1	CEF format version	CEF:0
Prefix2	Device vendor	Acronis
Prefix3	Device product	Detection and Response
Prefix4	Device version	3.16.11277.1618; 3.14.10275.1224
Prefix5	Signature ID (indicates the log type)	Detection and Response Monitoring Environment
Prefix6	Name	INFO
Prefix7	Severity	0
dvc	Detection and Response Server IP address	127.0.0.1
src	Source host address	26.75.120.157
shost	Source hostname	Not relevant to Detection and Response Monitoring Environment logs
spt	Source port	Not relevant to Detection and Response Monitoring Environment logs
suser	Source username	Not relevant to Detection and Response Monitoring Environment logs
msg	Content of the message	See the sample <i>msg</i> in the entry below

The following example shows the syntax of an entry in a Detection and Response Monitoring Environment Log:

```
Jun 26 18:03:39 host CEF:0|Acronis|Paranoid|2015.08.001.05|Detection and Response Monitoring Environment|INFO|0|dvc=172.21.0.122 src= shost= spt= suser= msg=Added a new policy: CCA_Explorer_DC_150418 username=\john action_category=\=Editing policies \| 2019-06-26 18:03:39
```

Configuring SAML Integration

SAML integration within Detection and Response enables you to pass authorization credentials to service providers for logging in to Detection and Response. This ensures users can log in to Detection and Response using SSO, rather than use separate login credentials.

SAML integration also enables you to manage users locally as you would using Active Directory or similar directory services; you can also apply permissions to users, according to the parameters defined in the configuration process described below.

To configure SAML integration

1. To get started with SAML integration, the SAML integration feature must first be enabled; contact Detection and Response support to enable this feature.
2. Log in to Detection and Response. At the top of the Detection and Response Monitoring Environment console, select **Server Management > Configure SAML Integration**. The SAML Integration Configuration dialog is displayed.

SAML Integration Configuration [X]

IDP Settings:
Select the IdP metadata file to import, or manually add/edit the below parameters.

Upload IdP Metadata File: [Choose file]

Manually Add/Edit Settings:

Entity ID: [Text Box]

Single Sign-on Service URL: [Text Box]

Logout URL: [Text Box]

IdP x509 Certificate: [Import file]

Attribute Name: [Permission_Level]

Permission Level Mapping:

Root: [ENT_D_Paranoid_Admin]

Admin: [ENT_D_Paranoid_Root]

Viewer: [ENT_D_Paranoid_Viewer]

Advanced Configuration:
The selected configuration is not secured enough

☐ Use Request ID
☐ Sign Request
☐ Sign Response

Export SP Metadata File: [Export]

[Apply] [Cancel]

Note

If the **Configure SAML Integration** menu option is not displayed, contact Detection and Response support.

3. Click **Export** to export the **metadata.xml** file. This file, which includes details and values from the Detection and Response Monitoring Environment console, should be sent to your organization's IT department.

Your IT department also needs to configure and export an SSO XML file, which includes the following local client parameters which Detection and Response needs for the authentication (handshake) process:

- Entity ID
- Single Sign-on Service URL
- Logout URL
- IdP x509 certificate
- Attribute name: Permission_Level

Note that the login process through SSO sends the details of the user who successfully logs in to Detection and Response. These details include the user name and permissions in the IdP.

However, because the permissions in the IdP system are different from the permissions in the Detection and Response system, the user permissions in the two systems should be mapped.

To perform the mapping, your IT department must define the attribute name of the permissions level as "Permission_Level"; the additional user permissions that come from the IdP are then mapped to the Detection and Response system permissions.

Note that the following three permission levels should be defined and mapped in Detection and Response.

- "ENT_D_Paranoia_Root" must be mapped to "Root"
- "ENT_D_Paranoia_Admin" must be mapped to "Admin"
- "ENT_D_Paranoia_Viewer" must be mapped to "Viewer"

After receiving the updated **metadata.xml** file from your IT team, continue with the configuration, as described in the following steps.

4. Click **Choose file** to import the XML file that your IT department created. After the import has completed, click **Apply**.

Ensure that the **Entity ID**, **Single Sign-on Service URL**, **Logout URL**, and **Attribute Name** fields are automatically filled. Note that you can also edit the fields manually, if required. The IdP x509 certificate should be provided in the XML file from your IT department, but can be uploaded manually (click **Import file** to upload the certificate).

5. In the **Permission Level Mapping** section, verify that the **Root**, **Admin**, and **Viewer** fields are automatically filled with the correct values:

- **Root:** ENT_D_Paranoia_Root
- **Admin:** ENT_D_Paranoia_Admin
- **Viewer:** ENT_D_Paranoia_Viewer

6. In the **Advanced Configuration** section, select from any of the following:

- **Use Request ID:** Select this option to enable the service provider to request the IdP to initiate authentication on its behalf via AuthnRequest.
- **Sign Request:** Select this option to validate the uploaded x509 certificate when verifying a request.

- **Sign Response:** Select this option to validate the uploaded x509 certificate when verifying a response.
7. Click **Apply**.
 8. To verify the SAML configuration, perform the following steps:
 - a. Log out of the Detection and Response Monitoring Environment console. You are immediately redirected to your client authentication page (according to the **Logout URL** defined in Step 3).
 - b. Log in as an SSO user.
If the log in is successful, you are redirected to the Detection and Response Monitoring Environment console as an SSO user.

Note

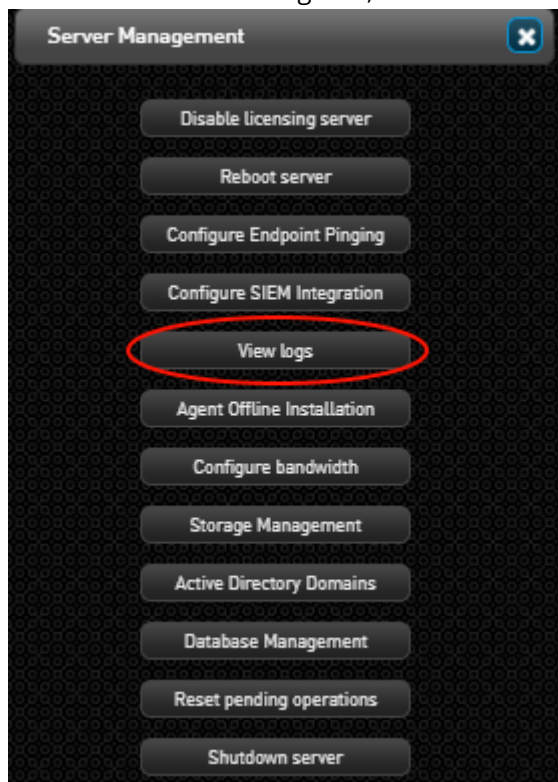
If there is an issue with the SSO client authentication, you can still access the Detection and Response Monitoring Environment console as a regular Detection and Response user. To do this, suffix `?skip_sso` to the client authentication page URL, as in the following example:

`https://hostname/?skip_sso`

If you connect as a regular Detection and Response user, we recommend you do not create additional users in Detection and Response beside your own.

Viewing and Downloading Log Files

The Detection and Response Monitoring Environment supports retrieval of any log file generated by the server, so you can view its contents, or download it and send the file to the Acronis Support team. To view a list of log files, click **Server Management** and select **View logs**.



The **Server Loggers View** dialog opens. From this dialog, you may view/download an individual log file, or download the entire collection of log files (by clicking **Download All**).



Retrieving a Single Log File

The upper portion of the **Server Loggers View** dialog allows you to view or download a specific selected log file. For convenience, the log files are organized in groups, according to type (Event logs, Activity logs, etc.) and are named according to date. You may view or download only one file at a time.

To view a log file, open the relevant **Logs** list, select the required file, and then click **View**.

The content of the selected log file is displayed in a popup window.



- To download a log file, open the relevant **Logs** list, select the required file, and then click **Download**.

The selected log file is exported to your **Downloads** folder.

Handling Agent Offline Installation

Under certain circumstances, such as heavy network congestion, it may be preferable to install the Agent locally rather than download an update package to endpoints from the server. Detection and Response's Agent Offline Installation feature enables you to create customized packages for local installation of the Agent on new endpoints or for local upgrade of Agents on existing endpoints.

An offline installation package always contains an Agent version. The following components may also be added to the package:

- BPM version
- List of Exceptions in the [Default Policy Set](#)

To avoid the need for additional configuration following installation, it is recommended to include these components when creating offline installation packages. When a package contains all relevant BPM versions and default policies, the Agent can begin working in the correct configuration immediately upon installation.

Agent Version Considerations

When you prepare an offline installation package, it is important to make sure that the Agent version in the package (desired target version) and the version assigned in the Group settings for the target endpoints are the same. If the package contains Agent version A, for example, and the Group that the Agent will be assigned to contains Agent version B, the offline installation will install version A. However, the server will then immediately update the Agent to version B (unless Update settings are disabled).

Note

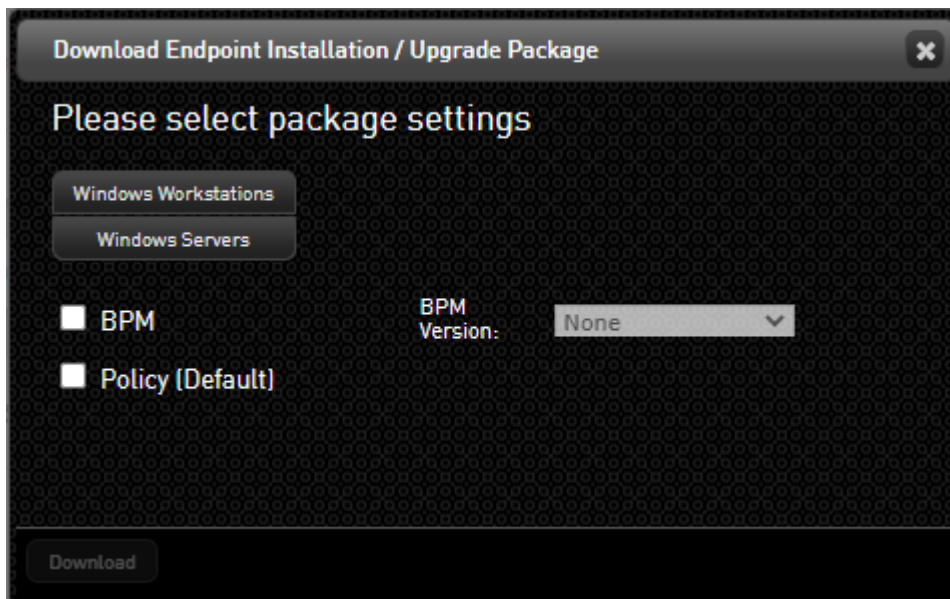
For details about assigning Agent versions and update settings for Groups, refer to [Configuring Settings for Groups](#).

When performing offline installation, to avoid version conflicts and successfully maintain the desired Agent version in the target endpoints, the following sequence is recommended as best practice:

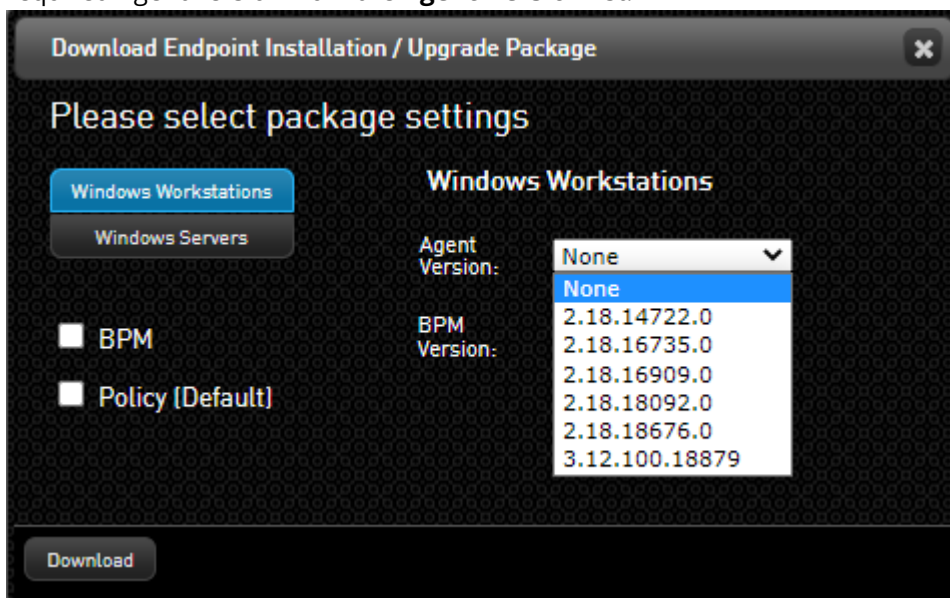
1. Decide which Agent version you want to install on the target endpoints.
2. In the **Endpoints Group** dialog of the relevant Group(s), set the **Updates** setting to **Disabled**. Then, change the Group's assigned Agent version to the version that will be contained in the offline installation package.
3. Create the offline installation package (see procedure below).
4. Install the Agent on the endpoint(s), using the offline installation package.
5. Following installation, go back to the **Endpoints Group** dialog and set the **Updates** setting to **Enabled**.

To perform Agent offline installation or upgrade:

1. From the Detection and Response Monitoring Environment console, click **Server Management** and select **Agent Offline Installation**.
The **Download Endpoint Installation/Upgrade Package** dialog opens.



At the top of the dialog, select **Windows Workstations** or **Windows Servers**. Then, select the required Agent version from the **Agent Version** list.



- 2.
3. To include a BPM version in the package, select the **BPM** checkbox. Then, select the required version from the **BPM Version** list.
4. To include the Default Policy Set in the package, select the **Policy (Default)** checkbox.
5. Click **Download**.

The offline installation package is created and stored in your **Downloads** folder.

To complete the installation or upgrade, extract the installation package on the endpoint, and run the appropriate batch file: **install_agent.bat** or **upgrade_agent.bat**

6.

			Local Disk	
..				
bpm.dll	756,564	756,564	Application extens...	6/7/2017 11:12
bpmg.dll	32,436	32,436	Application extens...	6/7/2017 11:12
bpmp.dll	9,184	9,184	Application extens...	6/7/2017 11:12
install_agent.bat	117	117	Windows Batch File	6/7/2017 11:12
server.conf.ok	17	17	OK File	6/7/2017 11:12
update_win7_x86_0.18.5670.1.exe	15,019,624	15,019,624	Application	6/7/2017 11:12
upgrade_agent.bat	126	126	Windows Batch File	6/7/2017 11:12

Managing Server Storage

The **Server Storage Management** dialog displays information about occupied storage space, and provides various options related to managing stored data and configuring storage alert settings. To open this dialog from the Detection and Response Monitoring Environment console, click **Server Management** and then select **Storage Management**.

Server Storage Management

Current disk usage:

Disk 0 (O/S): 88.7%

Disk 1 (Paranoid): 22.9%

Please select one or more cleanup operations to perform on the server:

<input type="checkbox"/> Action	Estimated Space	Disk 0 Usage	Disk 1 Usage
<input type="checkbox"/> Delete Automatic Database Backups	82.0 MB	0.00%	1.07%
<input type="checkbox"/> Delete Unused Agent And Bpm Packages	17.0 MB	0.00%	0.22%
<input type="checkbox"/> Delete Uploaded Database Backups	59.3 MB	0.00%	0.77%
<input type="checkbox"/> Delete Apache Logs	20.9 MB	0.37%	0.00%
<input type="checkbox"/> Delete Current Operating System Logs	154.0 MB	2.73%	0.00%
<input type="checkbox"/> Delete Old Operating System Logs	0.0 KB	0.00%	0.00%
<input type="checkbox"/> Delete Package Cache	2.3 MB	0.04%	0.00%
<input type="checkbox"/> Delete Temporary Files	21.7 MB	0.38%	0.00%
<input type="checkbox"/> Delete Uploaded Agent Logs	0.0 KB	0.00%	0.00%
<input type="checkbox"/> Delete Uploaded Extracted Agent Logs	0.0 KB	0.00%	0.00%
Total Selected:	0.0 KB	0.00%	0.00%

Run Storage Cleanup Remind me in 30 Minutes Ignore Configure

When the data in storage begins approaching maximum capacity, the dialog opens automatically to prompt users to perform a storage cleanup operation. Users can then select one of the following actions (at the bottom of the dialog):

- **Run Storage Cleanup:** Clears data from storage. For more information, refer to [Performing Server Cleanup](#).
- **Remind Me in <x> Minutes:** Closes the popup and opens it again after a defined, configurable period of time. For details about setting the time period, refer to [Configuring Cleanup Alert Settings](#) (below).
- **Ignore:** Closes the dialog and does not re-open it.
- **Configure:** Opens another dialog that allows you to modify the cleanup alert settings. For more information, refer to [Configuring Cleanup Alert Settings](#) (below).

Configuring Cleanup Alert Settings

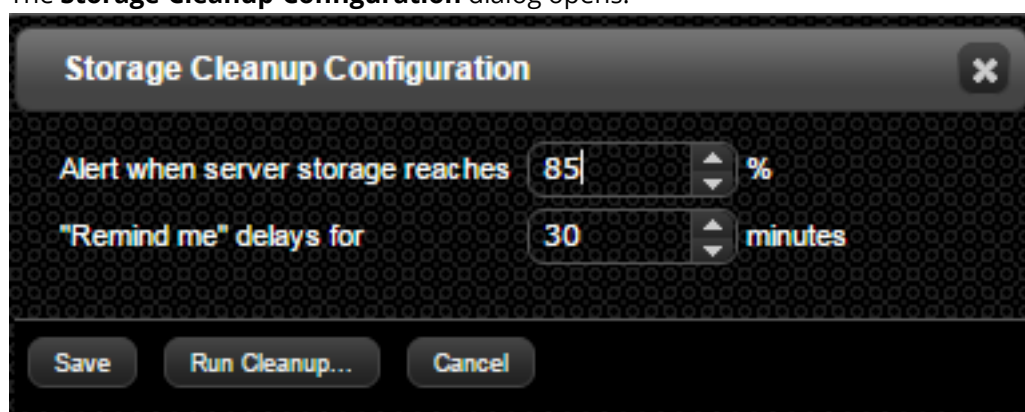
When data in storage begins approaching maximum capacity, the **Server Storage Management** dialog opens to alert users to the situation and prompt them to perform a cleanup operation. The following settings that trigger this cleanup alert are configurable:

- The percentage of consumed storage capacity that triggers the alert. The default value is 85%.
- The time interval after which the dialog opens again after a user clicks the **Remind me** button. The default value is 30 minutes.

To configure cleanup alert settings:

At the bottom of the **Server Storage Management** dialog, click **Configure**.

The **Storage Cleanup Configuration** dialog opens.



- 1.
2. Update the values as required.
3. Select one of the following options:
 - **Run Cleanup:** Re-opens the **Server Storage Management** dialog without saving the new settings.
 - **Save:** Saves your changes and re-opens the **Server Storage Management** dialog.

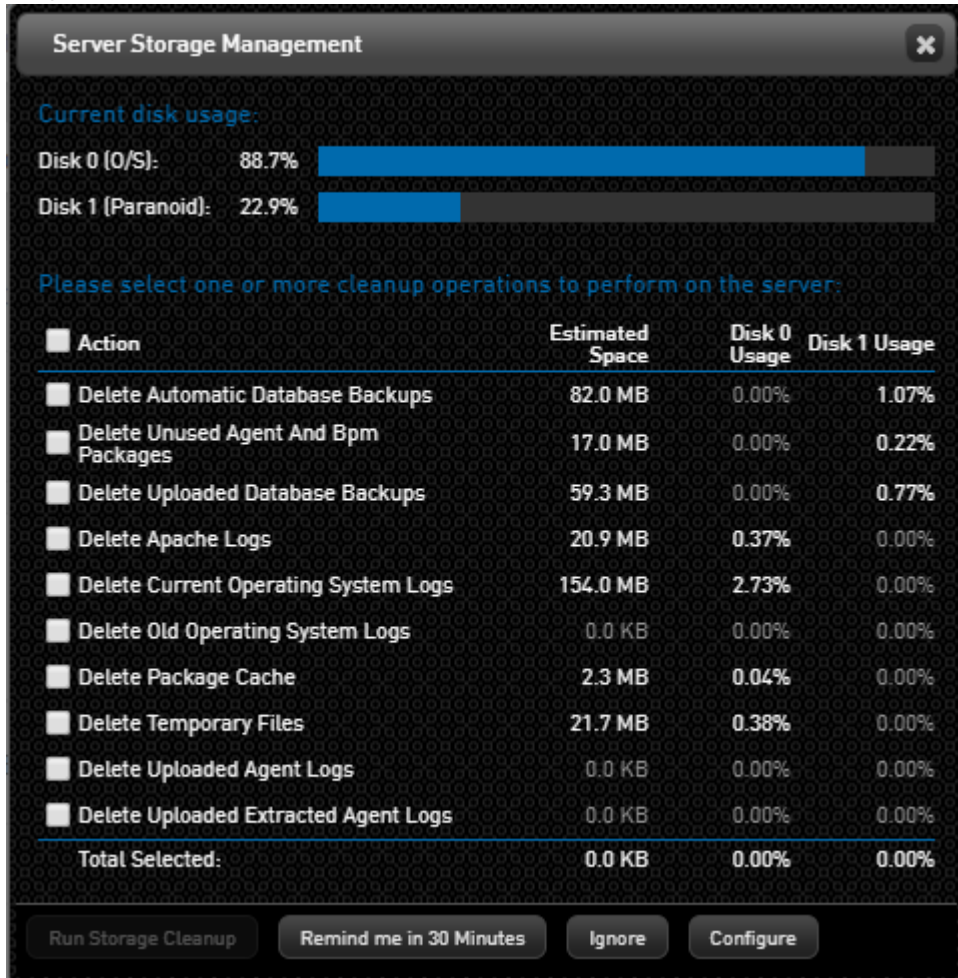
Performing Server Cleanup

The server cleanup operation involves selecting the files to clear from storage, and then running the cleanup.

To perform storage cleanup:

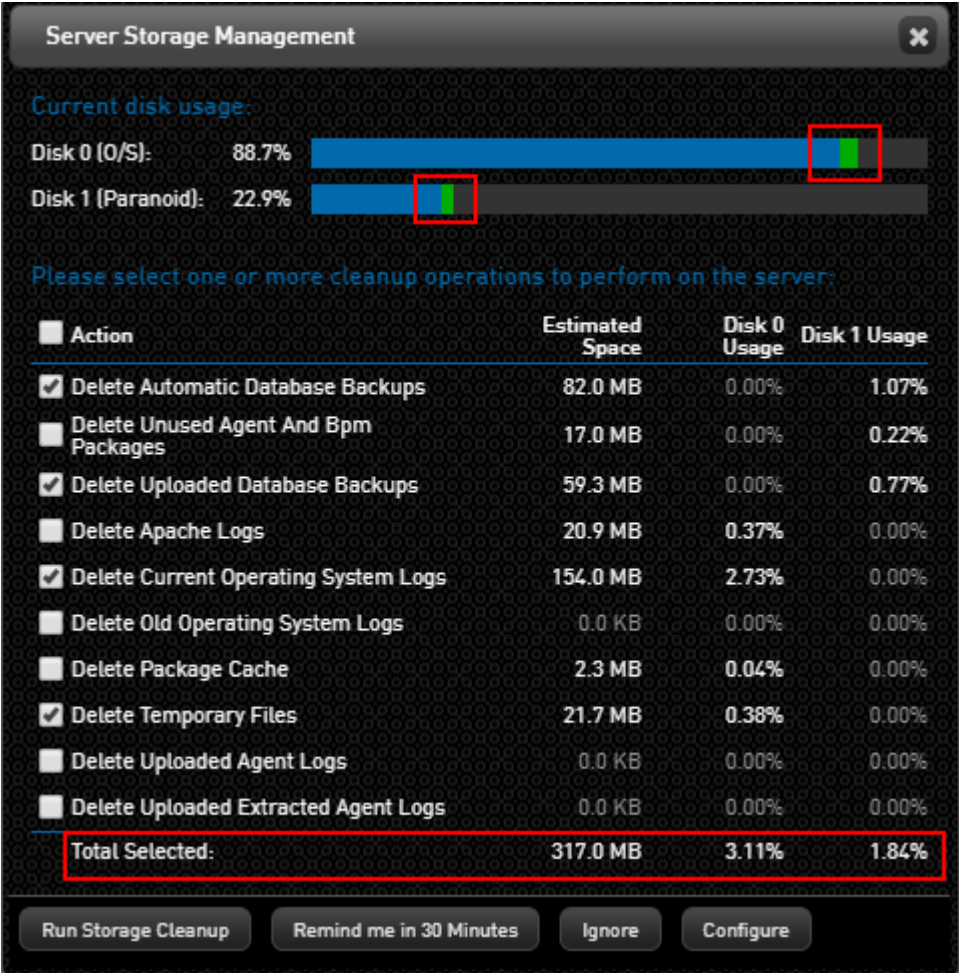
At the top of the Detection and Response Monitoring Environment console, select **Server Management > Storage Management**.

The **Server Storage Management** dialog opens. The bars at the top of the dialog indicate the percentage of occupied storage space for the operating system (Disk 0) and for Detection and Response (Disk 1).



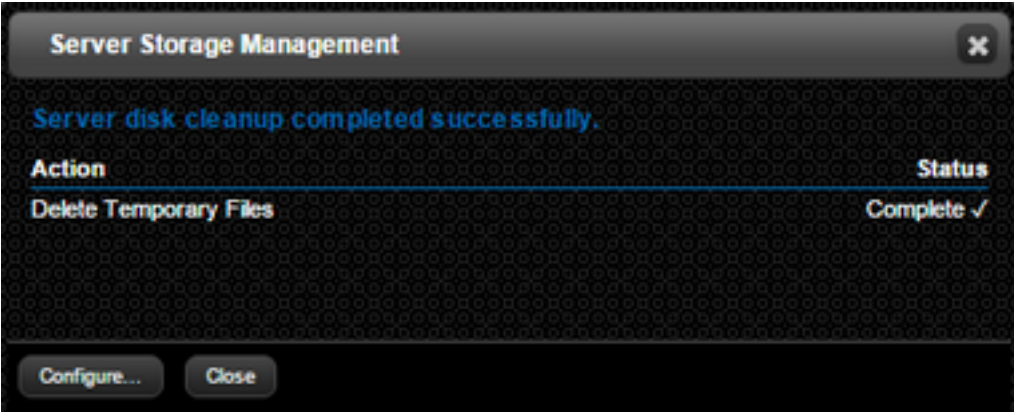
-
1. In the **Action** column, select the checkboxes of the items that you want to delete from storage. Clicking the checkbox next to the word **Action** automatically selects all the checkboxes.

As you make your selections, the amount of storage that will be freed is indicated on the bars in green. In addition, the sums of your selections are displayed below the list of actions.



At the bottom of the dialog, click **Run Storage Cleanup**.

When cleanup is complete, a confirmation message is displayed.



- 3.
4. Select one of the following options:
 - **Configure:** Allows you to modify the cleanup alert settings.
 - **Close:** Exits storage cleanup.

Handling Database Files

Detection and Response helps ensure adequate protection and backup of data by automatically creating a copy of the database every 24 hours. The five latest database files are kept accessible for administrative use, in case you need to perform exports, rollbacks, and so on. In addition, the Detection and Response Monitoring Environment lets you maintain optimal control of data by making extra backups, importing backups from other environments, and more.

All database management operations are performed from the **Database Management** dialog. To open the dialog from the Detection and Response Monitoring Environment console, click **Server Management** and select **Database Management**.



Name	Size	Date	
auto-20170614-062503	58M	2017-06-14 06:25	Actions ▼
auto-20170613-062502	58M	2017-06-13 06:25	Actions ▼
auto-20170612-062503	58M	2017-06-12 06:25	Actions ▼
auto-20170611-062503	58M	2017-06-11 06:25	Actions ▼
auto-20170610-062503	58M	2017-06-10 06:25	Actions ▼
uploaded_Nyotron_20170326-062502_ver_0_20_5829_0	57M	2017-04-24 13:52	Actions ▼
24APRLBEFOREUPLOAD	5.3M	2017-04-24 13:47	Actions ▼

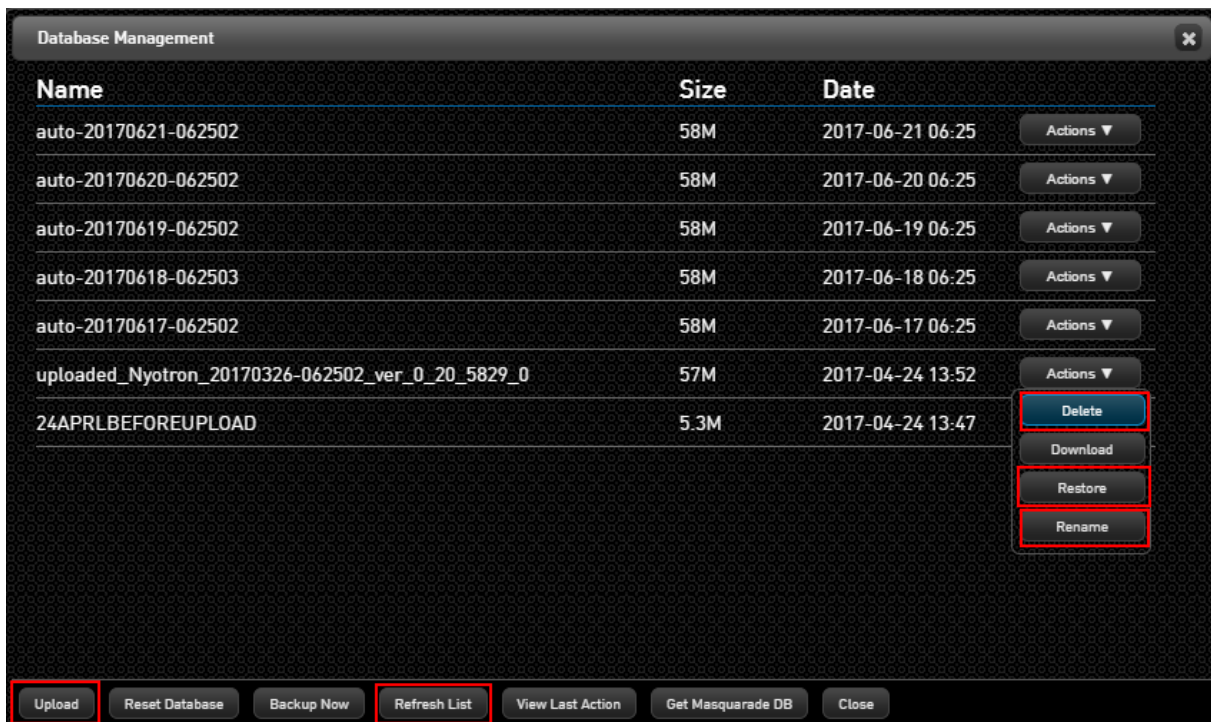
Upload Reset Database Backup Now Refresh List View Last Action Get Masquerade DB Close

The following sections explain how to:

- [Manage the database list](#) by uploading new files, deleting unnecessary files, and keeping the list up to date
- [Perform database backups](#)
- [Clear the database](#) using the Reset Database action
- [View database logs](#)

Managing the Database List

The following actions help keep the list of database files meaningful and current:



- **Upload:** Enables you to add a database file to the list.
- **Restore:** Overwrites the database content currently displayed with the content of another database file.
- **Refresh List:** Updates the database list with the latest information from the server. This action is relevant when there have been backend server changes done by Acronis Support.
- **Delete:** Removes a database file from the list.
- **Rename:** Enables you to update the name of a database file with a more relevant or friendly name.

To upload a database file:

At the lower left corner of the **Database Management** dialog, click **Upload**.

The **Upload Database** dialog opens.



1. Click **Browse** to access the **Open** dialog. Navigate to and select the relevant database file, and then click **Open**.
The name of the selected file appears in the field in the **Upload Database** dialog.
3. Click **Upload**.
A progress bar is displayed while the file uploads.

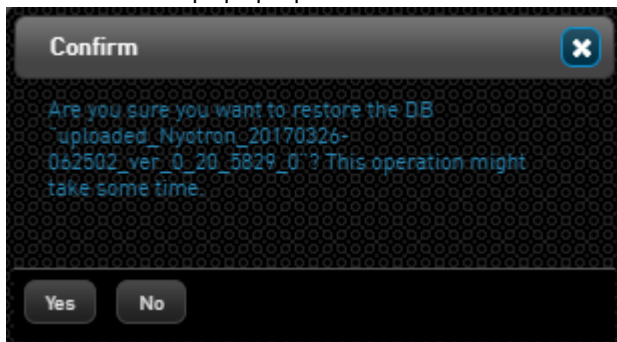
4. When the upload is complete, click **Close**.

The uploaded file is added to the list of backup files on the **Database Management** dialog.

To restore the Detection and Response Monitoring Environment with a backup database file:

From the **Database Management** dialog, in the row of the database file that you want to use for the rollback, click **Actions** and then select **Restore**.

A confirmation popup opens.



- 1.
2. Click **Yes**.

The Detection and Response Monitoring Environment database content is overwritten with the content of the selected database backup file.

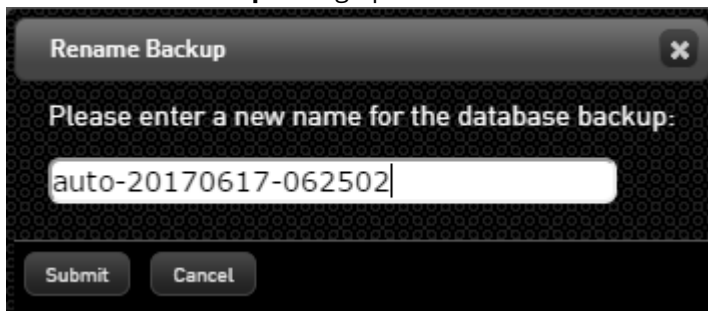
Note

Backup database files do not include various binary files related to Agent/BPM versions. (These files are stored on the server.) Therefore, version lists will appear after you restore the DB, but if the files they point to are not on the server, you will not be able to successfully assign Agent/BPM versions or perform other versioning operations.

To rename a database file:

From the **Database Management** dialog, in the row of the file that you want to rename, click **Actions** and then select **Rename**.

The **Rename Backup** dialog opens.



- 1.
2. Enter a new name in the field, and then click **Submit**. The name you enter must 2-32 alphanumeric characters. (Special characters are not supported.)

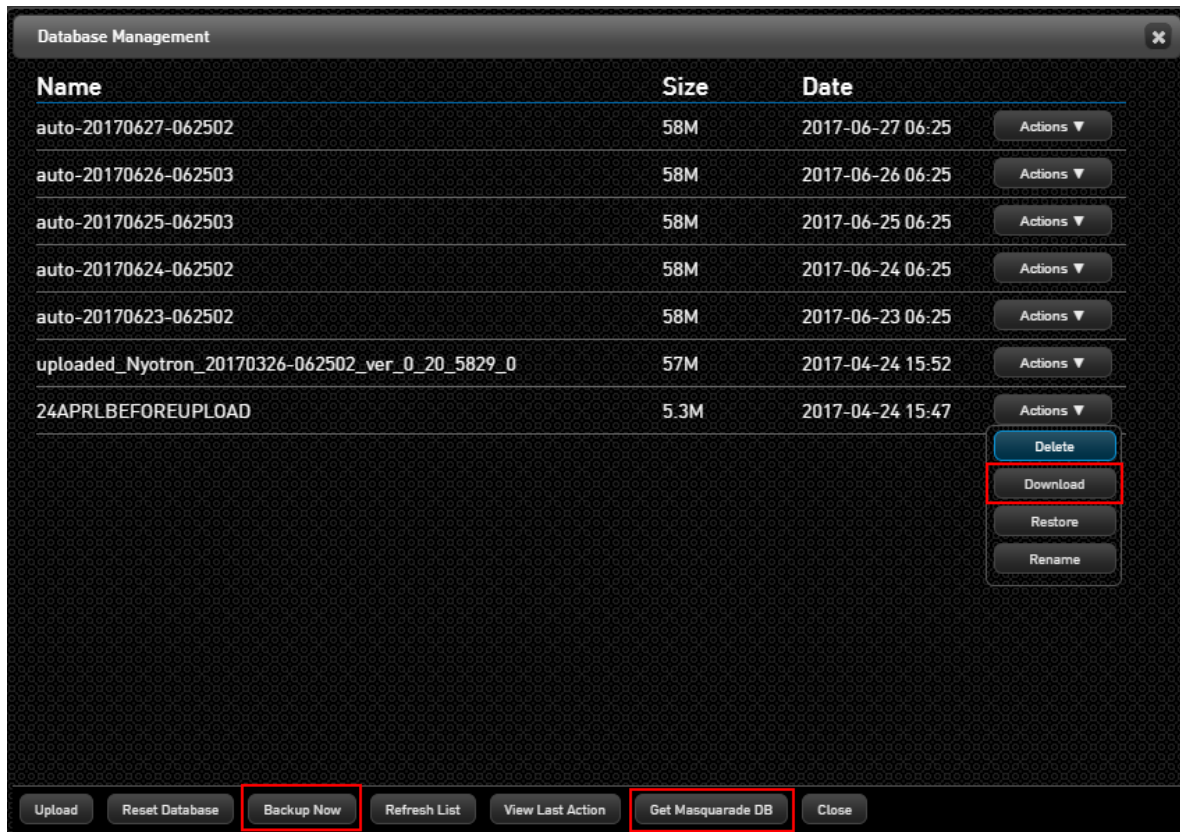
The new name appears in the list on the **Database Management** dialog.

Performing Database Backup

The following actions allow you to generate additional backup files:

- **Backup Now:** Creates a file containing the current database content.
- **Download:** Saves a selected database file in your **Downloads** folder.

Get Masquarade DB: Creates a file containing the current database content, with sensitive data masked.



The Backup Now and Get Masquarade DB actions create a new database file that is added to the list of files displayed on the **Database Management** dialog. You can then download the file and perform any other necessary actions on it.

To create a backup of the database:

1. At the bottom of the **Database Management** dialog, click **Backup Now** or **Get Masquarade DB**.

The **New Backup Name** or the **Masquarade Backup** popup opens, prompting you to enter a name for the file.



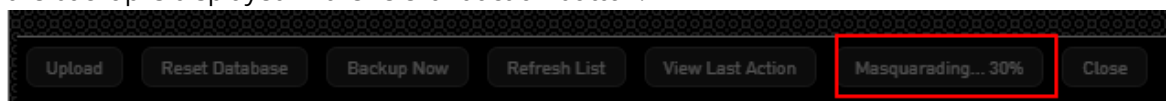
New Backup Name [X]

Please enter a name for the database backup:

Submit Cancel

Enter a name for the backup file, and then click **Submit**.

The backup process begins. During the backup, all action buttons are disabled. The progress of the backup is displayed in the relevant action button.



2.

When the backup is complete, the action buttons are enabled and the new backup file is listed on the **Database Management** page.

Clearing the Database

The Reset Database action clears the server's database content.

Caution

As the Reset Database action leads to loss of data, it is recommended that you use it with extreme caution.

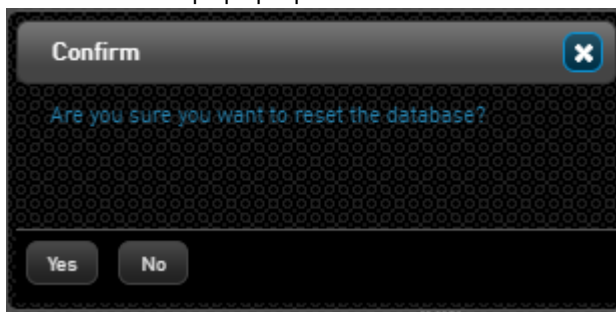
To clear the database:

At the bottom of the **Database Management** dialog, click **Reset Database**.



1.

A confirmation popup opens.

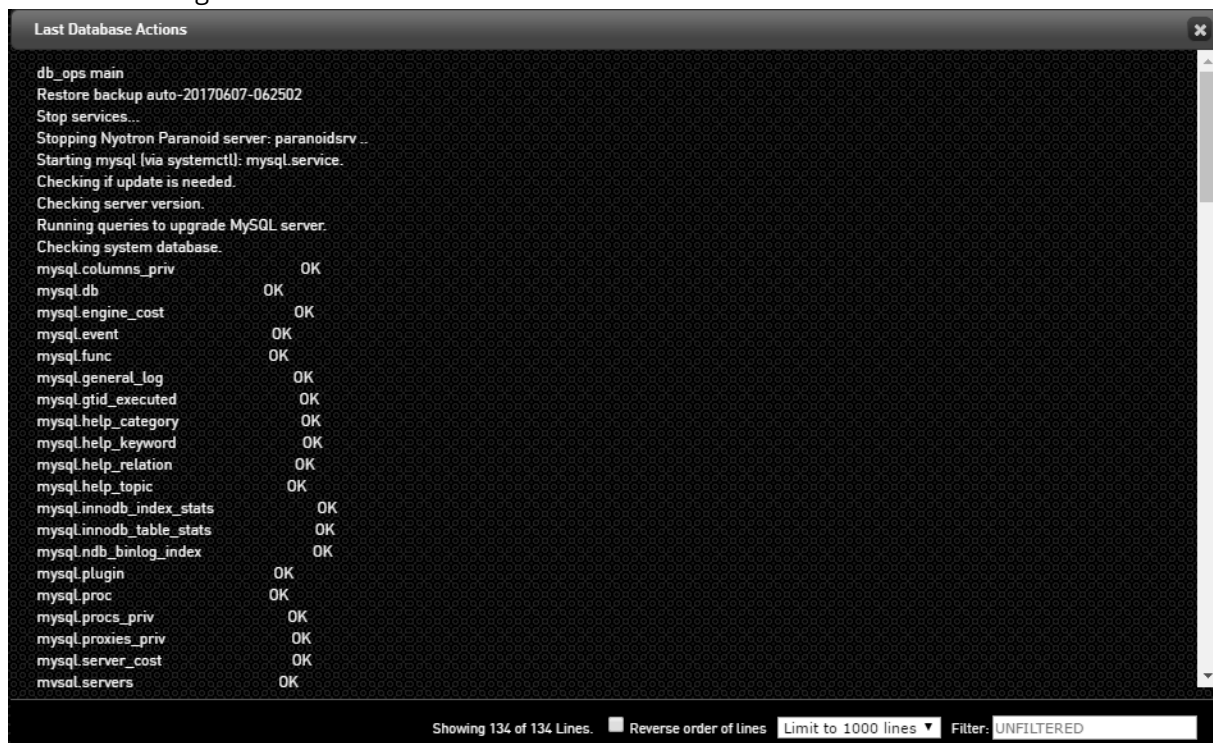


2. Click **Yes**.

Server database content is cleared.

Viewing Database Logs

Clicking the **View Last Action** button (at the bottom of the **Database Management** dialog) opens the **Last Database Actions** dialog. This dialog provides a log record of recent actions related to database management.



The filtering option enables you to search for relevant lines in the log according to keyword. The lines are automatically filtered according to the term entered in the **Filter** field. For example:

Last Database Actions

Starting mysql (via systemctl): mysql.service.
Running queries to upgrade MySQL server.
mysql.columns_priv OK
mysql.db OK
mysql.engine_cost OK
mysql.event OK
mysql.func OK
mysql.general_log OK
mysql.gtid_executed OK
mysql.help_category OK
mysql.help_keyword OK
mysql.help_relation OK
mysql.help_topic OK
mysql.innodb_index_stats OK
mysql.innodb_table_stats OK
mysql.ndb_binlog_index OK
mysql.plugin OK
mysql.proc OK
mysql.procs_priv OK
mysql.proxies_priv OK
mysql.server_cost OK
mysql.servers OK
mysql.slave_master_info OK
mysql.slave_relay_log_info OK
mysql.slave_worker_info OK
mysql.slow_log OK
mysql.tables_priv OK
mysql.time_zone OK
mysql.time zone leap second OK

Showing 33 of 134 Lines. ☐ Reverse order of lines Limit to 1000 lines Filter: mysql

Index

A

Acronis patented technologies 8

C

Configuring SAML Integration 196

Copyright statement 8