



ADMINISTRATOR GUIDE

Security Event Manager

Version 2024.2.1

© 2024 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

Table of Contents

SEM introduction	9
Introduction to SEM	9
About SEM reports	10
Integration with SolarWinds products	11
SEM components	12
SEM deployment example	12
About SEM Manager	13
About the SEM Agent	13
About network devices	14
About SEM reports	14
Log in to SEM	15
Log in to the SEM Console	15
Log in to the SEM CMC command line interface	16
License your SEM deployment	19
About SEM licensing	20
License a SEM evaluation	20
Run the Activate command	21
Recycle SEM licenses	23
Configure the settings and services	27
About the console settings	27
Start and stop the SEM appliance and agent	28
Enable log forwarding	30
Manage the SEM licenses	34
Download the debug logs	35
Set the date, time, and time zone on your SEM VM	35
Configure LDAP for SEM	37
Configure the Email Active Response connector	42
Enable SEM to receive SNMP traps	47
Send SNMP traps from SEM to other applications	48

Collect Windows Filtering Platform (WFP) events	51
Monitor SEM from NPM and the Orion Web Console using SNMP	52
Create a custom log in banner	55
Set the maximum email attachment size	56
(Optional) Set up SFTP connections to external systems	57
(Optional) Set up SMB file sharing to a Windows server	65
SEM Console	75
Dashboard	75
Live Events	75
Historical Events	75
Rules	76
Configure	76
SEM Dashboard	78
Available SEM widgets	79
Edit the SEM dashboard	82
Add dashboard widgets	83
Manage SEM users	95
Add SEM users	95
View system privileges associated with a role	99
Set the global password policy for SEM users	112
Set up Active Directory authentication in SEM	112
Set up single sign-on in SEM	118
Change the SEM CMC password	129
Monitor role users and filters	130
Collect event data from systems and devices	132
About SEM Manager and agent communications	132
Get started adding systems and devices to SEM	135
Configure SEM agents after the installation	137
Create connector profiles to manage and monitor SEM agents	140
Create a new connector profile	141
Add syslog and agent nodes to SEM	150
Update the SEM agents	152

Set up a separate syslog server for use with SEM	154
Manage the monitored nodes	155
Refine the node results	155
Edit a connector profile	156
Edit an Active Response connector profile	162
Update the SEM agents manually	166
Update the SEM connectors automatically	166
Add and remove agents from connector profiles	167
Configure Windows domain controller connectors	169
Verify USB Defender is installed on a SEM agent	170
Enable additional connectors to add extra log sources to SEM	170
Configure a firewall connector on SEM Manager	171
Verify the alias value associated with the connector	172
Export the SEM node information	173
Manage the SEM system resources	174
View the system resources	174
Allocate CPU and memory resources to the SEM VM	175
Manage the SEM data storage	180
View a disk usage event	185
SEM tuning and periodic maintenance tasks	185
Secure your SEM deployment	187
Review the SEM security checklists	187
Enable the security settings	188
Restrict SSH access to the SEM CMC interface	189
Create and manage tags	191
Sort the tag list by category	192
Filter tags by category	192
Filter tags associated with a query	193
Filter tags not associated with a query	195
Search for a tag	195
Add a tag	196
Delete a tag	197

Collect and normalize event data using SEM connectors	198
Configure SEM connectors for agent and non-agent devices	198
Apply a SEM connector update package	200
SEM connector categories	203
Microsoft SQL Server connector authentication methods	209
Monitor firewalls, proxy servers, domain controllers, and more	211
Monitor firewalls for unauthorized access	211
Monitor proxy servers for suspicious URL access	217
Monitor antivirus software for viruses that are not cleaned	219
Enable Windows file auditing for use with SEM	221
Configure the Windows audit policy for use with SEM	223
Configure the USB Defender local policy connector in SEM	228
Monitor Microsoft SQL databases for changes to tables and schemas	229
Monitor Windows domain controllers for brute force hacking attempts	231
Track Cisco buildup and teardown events	237
Monitor Windows files, directories, and registry settings using FIM connectors	239
Start a FIM driver	239
Add a FIM connector to a node	241
Create a FIM connector configuration	243
Configure a FIM connector from a template	244
Edit a FIM connector configuration	247
Create FIM file and directory inclusions	248
Create FIM file and directory exclusions	250
Create FIM registry inclusions	251
Create FIM registry exclusions	253
FIM advanced connector settings	254
Configure user defined groups	256
How rules and filters use user-defined groups	256
Create or edit a user-defined group	257
Edit a user-defined group	262
Customize the blank and sample user-defined groups included with SEM	262
About SEM groups	263

Import user-defined group elements	266
Export user-defined group elements	268
Configure directory service groups in SEM	269
Create event groups	272
Create time of day groups	280
View live and historical events	292
Live Events view	292
Analyze historical data	320
Set the live and historical event limits	358
Configure the occurrence settings	359
Edit the expressions	360
About the event types	360
Create rules that respond to security events	434
Get started building custom rule expressions in SEM	434
About SEM rules	434
Create a new rule	436
Configure the occurrence settings	443
Edit the expressions	444
Create a rule from a rules template	444
Create a rule from a filter	446
Test, enable, and disable rules in SEM	447
Import and export SEM rules	453
Create email templates for use with SEM rules	457
Example SEM rules	460
Create response actions for network and system events	470
About SEM response actions	470
Use computer-based active responses in SEM	483
Use the Append Text to File active response in SEM	484
Configure an active response connector on a SEM agent	485
Use the Block IP active response in SEM	487
Configure the Detach USB Device active response in SEM	489
Configure the Disable Networking active response in SEM	490

Configure the Kill Process active response in SEM	492
Create regulatory and compliance reports	495
About SEM reports	495
Set up the SEM reports	497
Run or schedule a SEM report	498
Locate migrated SEM audit reports	508
About the CMC	522
About the CMC command line	522
CMC main menu	523
CMC appliance menu	524
CMC manager menu	526
CMC service menu	528
CMC rawlogs menu	530
Troubleshoot your SEM deployment	532
Troubleshoot alerts in the SEM Console	532
Troubleshoot SEM agents and network devices	536
Troubleshoot network and syslog device logging in SEM	539
Glossary of SEM terms	543

SEM introduction

This section provides an overview of Security Event Manager (formerly Log & event Manager), including information about audit reports and integrating the application with SolarWinds products.

Introduction to SEM

SolarWinds Security Event Manager (SEM) is a security information and event management (SIEM) virtual appliance that collects and normalizes log data generated across an entire network into one central location. After the log data is collected, you can use the SEM Console to:

- Identify patterns displayed in the dashboard that may indicate suspicious activity.
- View live events in real time.
- View historical events for forensic analysis and troubleshooting.
- Create a rule to monitor event traffic and trigger an automated action when a defined event or events occur. These automated actions can include stopping processes, detaching USB devices, blocking IP addresses, logging off users, and sending emails to support teams.

SEM collects log data in a network from two resources:

- Agents
- Non-agent devices

Agents

Agents are software applications that gather hardware and software information. This information is sent back to a monitoring system to track these assets.

Similarly, the SEM Agent collects log data on devices that cannot send their own logs to SEM. The agent normalizes the log data into a format that SEM can understand. When normalization is completed, the data is processed and converted to charts and graphs in the SEM Console.

See [About the SEM Agent](#) for more information.

 You can use SolarWinds Patch Manager to schedule patching for your SEM agents. See [How to Schedule Patching for Security Event Manager Agents](#) for details.

Non-agent devices

Non-agent devices collect and send log data directly to SEM for normalization and processing. This data is converted to charts and graphs in the SEM Console. Because the log data is in a format that SEM can understand, no agent is required.

SEM policy engine

When the normalization is completed, SEM processes the data. The SEM policy engine correlates the data based on user-defined rules and local alert filters, and then initiates the associated actions when applicable. These actions can include:

- Notifying users through the console or by email
- Blocking an IP address
- Shutting down or rebooting a workstation
- Passing alerts to the SEM database for future analysis and reporting within the Reports application

Agent installation

You can install agents on workstations, servers, and other network devices. Agents can send log data from security products (such as antivirus software and network-based intrusion systems) on each device to the SEM virtual appliance.

If you cannot install an agent on a device (such as firewalls and routers), you can configure the device to send log data to the SEM Manager for normalization and processing. If your change management process does not permit adding any additional syslog servers to the network device configurations, you can leverage your existing syslog servers.

About SEM reports

You can [create regulatory and compliance reports](#) from the [Historical Events screen](#) located in the Historical Events & Reports tab. The reports convert historical event search queries into information you can use to troubleshoot and identify problems in your organization.

After you [set up the reports](#), you can [run or schedule a report](#) on a predefined or customer search query to view events and trends that help you make informed decisions about your network activity. All reports can be saved in CSV or PDF format.

SEM includes predefined search queries to help you get started. You can also [create search queries](#) using the intuitive search builder.

If your reports exceed your email attachment requirements, you can [set up a secure file transfer protocol \(SFTP\) connection](#) to one or more external Microsoft Windows servers in our organization. This option allows you to automatically deliver your reports directly to a Windows server in your organization that your stakeholders can access from their systems.

Integration with SolarWinds products

Additional SolarWinds solutions, such as [Network Performance Monitor \(NPM\)](#), [Server & Application Monitor \(SAM\)](#), and [Virtualization Manager \(VMan\)](#), can send performance alerts as SNMP Traps to the SEM Manager to correlate performance alerts with SEM events.

See [Configure the settings and services](#) for instructions on how to configure SEM to interact with the other systems and services in your IT environment. These instructions include:

- [Enable log forwarding](#)
- [Enable SEM to receive SNMP traps](#)
- [Send SNMP traps from SEM to other applications](#)
- [Collect Windows Filtering Platform \(WFP\) events](#)
- [Monitor SEM from NPM and the Orion Web Console using SNMP](#)

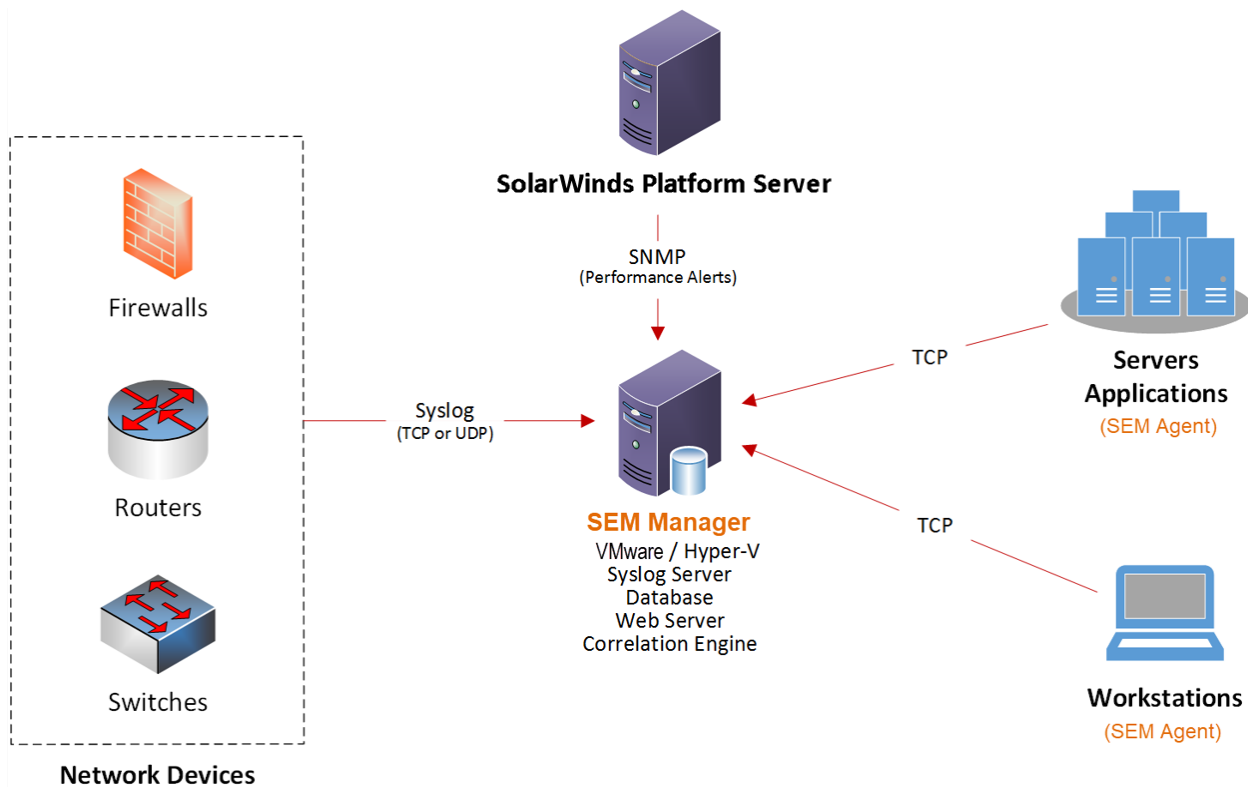
 SEM uses additional data collection tools, including Web Services and SNMP traps. Contact [SolarWinds Support](#) for more information about integrating SEM into your corporate enterprise.

SEM components

This section describes the software components that comprise a typical SEM deployment and how you can deploy SEM in your network.

SEM deployment example

The following illustration highlights the software components, log files, and network protocols in a typical SolarWinds SEM deployment.



A complete SEM installation includes the following components:

- **SEM Manager (or SEM VM):** Collects and processes log and event information. This component is installed first.
- **Desktop software or web user console:** Allows you to view your SEM deployment from a desktop or laptop computer. If your SEM deployment is integrated with the SolarWinds Platform, the web console is installed on the SolarWinds Platform server.

When the integration is completed, you can access the web console at:

`http(s)://<semhost>/webui`

About SEM Manager

SEM was initially marketed and sold as a physical appliance that is deployed on a network. Today, the SEM Manager is the virtual image of a Linux-based appliance. You can install the SEM Manager Virtual Machine (VM) on a host computer running a VMware vSphere or Microsoft Hyper-V hypervisor. You can also install SEM Manager in the cloud.

 The SEM documentation uses the term virtual machine (or VM) to refer to the SEM virtual appliance that runs on a hypervisor, such as Microsoft Hyper-V and VMware vSphere.

The SEM Manager collects and processes log and event information. This information includes data received from the following systems and services:

- Hardened Linux operating system
- Syslog Server and SNMP Trap Receiver
- High compression, search-optimized database
- Web server
- Correlation engine

About the SEM Agent

The SEM Agent is installed on workstations, servers, and other network devices. The agent collects and normalizes log data in real time before it is sent to the [SEM Manager](#). By default, the agent also collects security data (such as Windows application, Windows system, and Windows security event logs) and transmits that data over TCP to the SEM Manager.

The Windows Security connector tracks 100% of the event logs by default. This is because the Windows application and Windows system logs can also receive other application logs, such as antivirus logs. In this example, logging is not enabled by default and must be configured.

For example, if you are running McAfee Antivirus (which may write to the Windows Application log), the Windows Application connector will not read these events. Instead, the McAfee connector will read and normalize these events because they are vendor specific and not a Windows log event. This method also applies to Printer logging, Internet Information Services (IIS) logging, Windows Server Update Services (WSUS) logging, and so on.

The SEM agent creates a small footprint on the device and prevents log tampering during data collection and transmission. You can also use the SEM agent with devices that support syslog. The agent transmits syslog messages over TCP to the SEM Manager. TCP is preferred over UDP because TCP ensures that all messages arrive intact.

The SEM agent provides the following benefits:

- Captures events in real time.
- Encrypts and compresses the data for efficient and secure transmission to the SEM Manager.
- Buffers the events locally if you lose network connectivity to the SEM Manager.

About network devices

The following table lists the network resources that provide input to SEM Manager.

Network resource	SEM input
Network Device log sources (such as routers, firewalls, and switches)	Syslog messages
Servers and applications	SEM agent data
Microsoft Windows workstations	SEM agent data
SolarWinds NPM	SNMP traps (performance alerts)
SolarWinds SAM	See Enable SEM to receive SNMP traps for details.
SolarWinds VMAN	

SEM accepts device input using the TCP and UDP protocols. For example:

- Network devices use TCP or UDP to send syslog events to the SEM Manager.
- SEM agents installed on servers and workstations use TCP to push data to the SEM Manager.
- [SolarWinds Platform](#)/VMAN server instances (including NPM and SAM) send SNMP traps over UDP to the SEM Manager.

About SEM reports

The SEM reports convert historical data queries into information to help you troubleshoot and identify network problems. You can run several [query reports](#) in the [Historical Events and Reports](#) tab to view events and trends that help you make informed decisions about your network security.

Log in to SEM

This section describes how to log in to the SEM user interfaces.

Log in to the SEM Console

1. Open a [supported web browser](#) window.
2. In the address bar, enter the following URL and then press Enter:

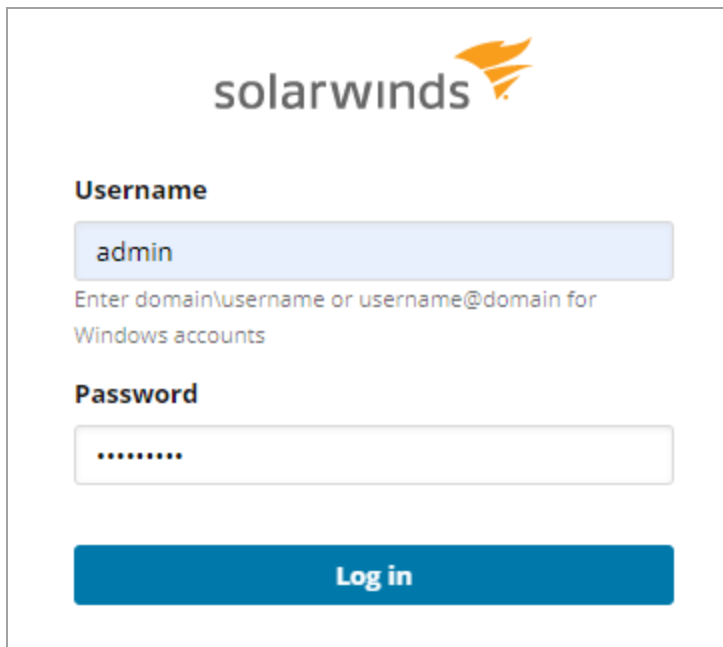
`https://<appliance-ip-or-hostname>`

where `<appliance-ip-or-hostname>` is:

- The IP address or hostname of your Microsoft Hyper-V or VMware vSphere appliance
- The hostname of your Microsoft Azure, Azure CLI 2.0, or Amazon Web Services deployment

3. In the SEM Console Login screen, enter your user credentials.

 If SSO is enabled, you can log in by clicking Log in with SSO and using your Windows credentials.



- a. In the Username field, enter your user name (for example, `admin`).

- b. In the Password field, enter your user password.
4. Click Log in.

Log in to the SEM CMC command line interface

Use the CMC command-line interface (CLI) to perform administrative tasks such as:

- Rebooting or shutting down the SEM VM
- Upgrading the SEM Manager software
- Applying connector updates
- Deploying new connector infrastructure to SEM Managers and Agents

There are two ways to log in to the CMC CLI:

- Connect using the console provided with your hypervisor
- Connect using a secure shell (SSH) client such as PuTTY

CMC Access Restrictions

The following access restrictions apply to the CMC command-line interface:

- You do not need an account with root access to administer SEM from the CMC command line.
- You need to enter the CMC user name and password to log in to the CMC command line using SSH. The user name is `cmc` and the default CMC password is `password`. See [Change the SEM CMC password](#) to change it.
- You need to enter the CMC username and password to login via the hypervisor console in Hyper V and VMWare.
- SSH access to the CMC interface can be restricted by IP address or host name. If enabled, this security feature blacklists everyone from logging in to the CMC interface except those users who connect from an explicitly allowed IP address or host name. See [Restrict SSH access to the CMC interface](#) for details.

Log in to the CMC command-line interface using the hypervisor virtual console

 See your hypervisor documentation for information about using the virtual console.

1. Open your hypervisor and connect to the SEM VM:

For VMware vSphere:

- a. Click the Console tab.
- b. Select Advanced Configuration on the main console screen, and press Enter to access the command prompt.

For Hyper-V:

- a. Click Action > Connect, and then click the Console tab.
- b. Use the arrow keys to navigate to Advanced Configuration, and press Enter.

2. Enter the CMC user name and password.

The CMC menu appears with a `cmc>` prompt.

Next steps:

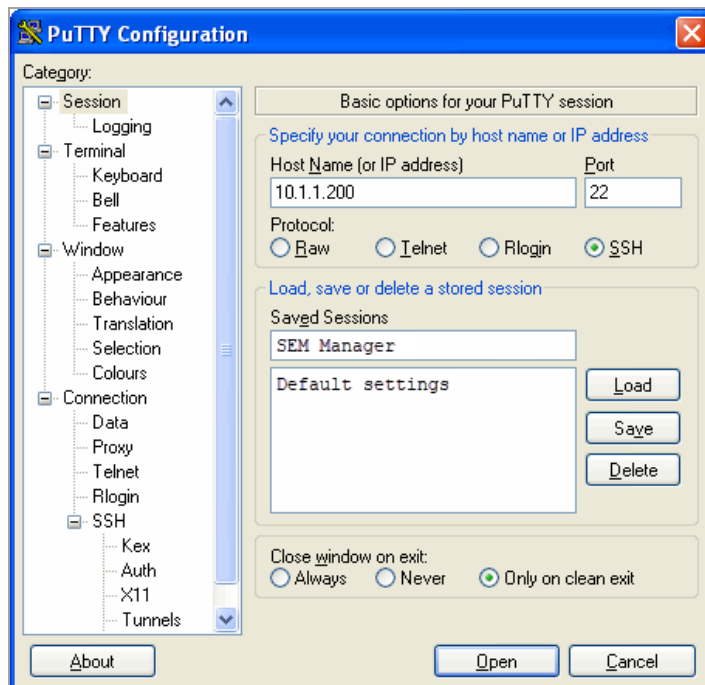
- See [About the CMC](#) for a list of supported commands.

Log in to the CMC command-line interface using SSH

 See [CMC access restrictions](#) for information about credentials and SSH access restrictions.

You can connect to SEM using a secure shell (SSH) client (such as PuTTY). The following steps show how to configure PuTTY to open the CMC command line, but these settings will work in any SSH client.

1. Open PuTTY and verify that Session is selected in the Category section.



2. Enter the following:

- Host Name (or IP address) – Enter the IP address of the SEM VM. In this example, the IP address is 10.1.1.200.
- Port – Enter 22.
- Protocol – Select SSH.
- Saved Sessions – Enter `SEM Manager`, and then click Save.

3. Click Open.



The next time, double-click SEM Manager in the Saved Session box to open the connection.

4. Log in to the appliance:

- At the log in as prompt, type `cmc`, and then press Enter.
- At the password prompt, type your password, and then press Enter.

 The default CMC password is `password`. See [Change the SEM CMC password](#) to change it. For help recovering a lost CMC password, contact SolarWinds Support.

The `cmc>` prompt opens with a list of available commands.

See [About the CMC](#) for a list of supported commands.

```

////////////////////////////////////
///      SolarWinds Security Event Manager      ///
///                               management console                               ///
////////////////////////////////////

Detected VMware Virtual Platform
Product Support Key: 7 2 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Available commands:
[ appliance ] Network, System
[ manager ]   Upgrade, Debug
[ service ]   Restrictions, SSH
[ rawlogs ]   Raw logs Configuration/Maintenance
upgrade      Upgrade this Appliance
help         display this help
exit         Exit
cmc >

```

License your SEM deployment

You can view your license information in the Settings window. To access, click the System icon  in the toolbar and then select Manage License.

In the Manage license window, you can view, upgrade, activate, and deactivate your SEM license. If you do not have a license or your license is inactive, Activate license is displayed in the window. Only administrators can upgrade, activate, and deactivate a license.

 The System icon  may vary depending on whether your license is active or inactive.

Settings

AUTHENTICATION	MANAGE	RECYCLE
EVENTS LIMITS	License type:	Evaluation Activate license
IMPROVEMENT PROGRAM	Maintenance license expiration:	(20 days left)
LOG FORWARDING	Total nodes:	15500
LICENSE	Used universal licenses:	803 / 7500
SYSTEM RESOURCES	Used workstation licenses:	0 / 0
THREAT INTELLIGENCE	License key:	N/A
UPDATES	Name:	visual tester
WEB CONSOLE	Email:	visual.testster@email.com
SECURITY	Phone:	777555333
SHARING		

If you do not have a license key, click Purchase license key. SEM directs you to the available licensing options located on the SolarWinds website.

See [SEM license activation](#) to activate your license online or offline.

See [Update the SEM license](#) to update your license.

After you activate your license, the Manage license window displays your license information with options to upgrade or deactivate your license.

License type:	Security Event Manager SWE8000 for SEM7500	Upgrade license Deactivate
Maintenance license expiration:	(204 days left)	
Total nodes:	15500	
Used universal licenses:	803 / 7500	
Used workstation licenses:	247 / 8000	
License key:		
Name:	visual tester	
Email:	visual.testers@email.com	
Phone:	777555333	

About SEM licensing

Licensing a Security Event Manager deployment is based on two license types:

- Universal license (SEM)
- Workstation Edition license (SWE)

A **Universal license (SEM)** includes the number of universal nodes. Universal nodes include non-agent devices, such as switches, routers, and firewalls, and systems running either a Windows Server or Unix operating system. For example, a SEM deployment with a SEM150 subscription can add 150 universal nodes.

A **Workstation Edition license (SWE)** includes the number of workstation nodes. Workstation nodes include desktop systems that run Windows for Workstations and the SEM Agent. For example, a SEM deployment with a SWE250 subscription can add 250 Windows workstation nodes.

Contact [SolarWinds Sales](#) for a license type that supports the number of nodes you want to monitor in your deployment.

License a SEM evaluation

If you are evaluating SEM, you do not need to apply an activation key to activate the SEM VM. For 30 days, you will have unlimited access to all product features.

If you have not purchased and provided a license key after 30 days, the application will stop collecting event logs from your syslog and agent devices. You can continue using SEM in this mode and access your saved logs. [Applying a license](#) reactivates event log collection and you can continue monitoring all events in your deployment. If you need to extend your evaluation period, contact [Customer Sales](#).

You can upgrade to a fully-functional production version by purchasing a new license from [Customer Sales](#) and downloading the license key from the [Customer Portal](#). After you [install the new license key](#), you can access all features within the SEM appliance.

 You cannot upgrade your license using the SolarWinds License Manager.

Run the Activate command

After you install the license, run the Activate command to help secure SEM from unauthorized users.

 You can still evaluate SEM without running the activate command. You can also turn off HTTP.

The activation procedure prompts you to:

- Configure a static IP address and hostname for the SEM VM
- Configure a secure password
- Verify your network configuration
- Specify a list of IP addresses that can access SEM reports (optional)
- Export the SSL certificate that ensures secure communications between the SEM desktop console and the SEM Manager

 Port 8080 is unsecure and is automatically disabled after activation has been completed. Port 8443 is always available.

Prepare to run the Activate command

If you plan to use the SEM desktop console, copy the SEM CA SSL certificate to the Trusted Root Certification Authorities certificate store prior to running the Activate command.

 By default, SEM uses a pre-made, self-signed certificate.

When the activation is complete, the SEM VM automatically exports the SSL certificate. The SEM desktop console connects with the SEM Manager using secure communications on port 8443.

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

The default password is `password`.

2. At the `cmc>` prompt, type:

```
manager
```

3. Export the CA certificate so that you can import it into a computer running the SEM console.

At the `cmc::manager>` prompt, type:

```
exportcert
```

4. Follow the prompts to export the SEM Manager CA certificate.

An accessible network share is required. Once the export is successful, you will see the following message:

```
Exporting CA Cert to \\server\share\SWICAer -hostname.crt ... Success.
```

5. Locate and double-click the certificate on the network share.
6. Click Next.
7. Select Place all certificates in the following store, and then click Browse.
8. Select Trusted Root Certification Authorities.
9. Click OK, and then click Next.
10. Click Finish.
11. Click Yes to confirm that you trust the certificate.

Run the Activate command

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

The default password is `password`.

2. Configure SEM to use a static IP address.



SolarWinds recommends configuring a static IP address for the SEM VM. If you use DHCP instead and your IP address changes, your deployed Agents may be disconnected and require additional troubleshooting to resolve.

- a. At the `cmc>` prompt, type `appliance`, and then press Enter.

The prompt changes to `cmc::appliance>` to indicate that you are in the appliance configuration menu.

- b. Type `activate`, and then press Enter.

The Activation splash screen appears.

- c. Press Enter to go to the next screen.

- d. When prompted, select Yes to configure a static IP address for the SEM VM.
- e. At the `cmc::appliance>` prompt, type `netconfig`, and then press Enter.
- f. At the prompt, type `static`, and then press Enter.
- g. Follow the steps on your screen to configure the Manager Appliance network parameters.

i Be sure to enter a value for each prompt. Leaving blank entries results in a faulty network configuration that requires you to rerun `netconfig`.

- h. Record the IP address assigned to the SEM VM. You will use this IP address to log in to the SEM console.
3. When prompted to change the hostname, select Yes to specify a hostname or No to accept the default hostname. To specify a hostname, use the following naming conventions:
 - Hostname labels can only contain the following:
 - ASCII letters A through Z (letters are not case sensitive)
 - Digits 0 through 9
 - Hyphens (-)
 - Hostnames cannot start with a digit or a hyphen, and must not end with a hyphen.
 - No other symbols, punctuation characters, or white spaces are permitted.
 4. When prompted to specify a list of IP addresses that can access reports, SolarWinds recommends selecting Yes.
 5. Confirm your network configuration.
 - a. At the `cmc::appliance>` prompt, enter:

```
viewnetconfig
```

i To ensure secure communications between SEM and the SEM desktop console, the SEM VM automatically exports an SSL certificate when the activation completes. Following activation, the SEM desktop console securely connects with the SEM VM on port 8443.

- b. Follow the prompts to export the certificate to a network share.

Recycle SEM licenses

License recycling allows you to collect and reuse your [subscription or perpetual SEM licenses](#) from [monitored nodes](#) that have not sent an event to the SEM manager within a specified amount of time.

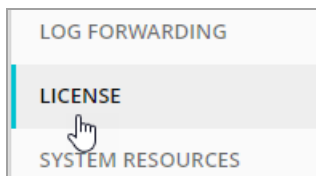
This feature helps you minimize your IT software expenses by maximizing your [Universal \(SEM\) and Workstation Edition \(SWE\)](#) license pools. Using License recycling, you can repurpose your SEM licenses to collect log data, monitor event traffic, and view historical events from only active non-agent devices and workstations in your deployment.

Set up license recycling

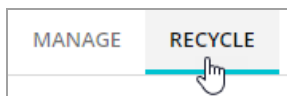
1. [Log in to the SEM console](#) as an administrator.
2. Open Settings.



3. In the left column, click License.

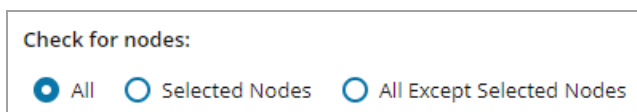


4. Click the Recycle tab.

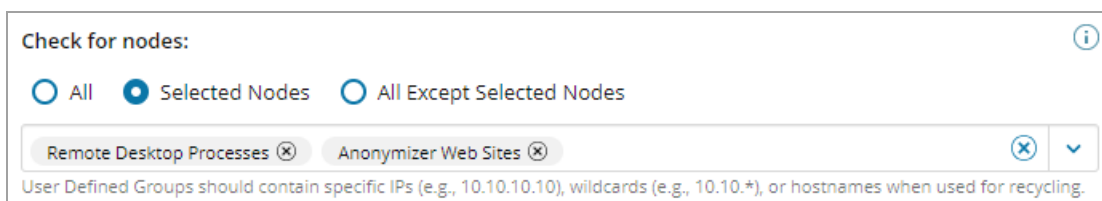


5. Select the [monitored nodes](#) you want to check for recycling.

Select All to check all available nodes.



Select Selected Nodes to check the nodes in defined groups that you select from the drop-down menu. Your selections display in the drop-down menu field.



Select All Except Selected Nodes to check all nodes except for the nodes in defined groups that you select from the drop-down menu. Your selections display in the drop-down menu field.

Check for nodes:

☐ All
☐ Selected Nodes
☒ All Except Selected Nodes

Remote Desktop Processes
Anonymizer Web Sites

User Defined Groups should contain specific IPs (e.g., 10.10.10.10), wildcards (e.g., 10.10.*), or hostnames when used for recycling.

6. Select the amount of time to pass before SEM recycles the license of the node.

Recycle license if a node is offline and has not sent an event for more than:

3
Weeks

Last execution: never

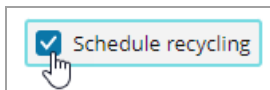
7. To create a license recycling schedule, go to the next step.

To recycle the SEM license on all selected nodes now, click Recycle now.



8. Create a schedule to recycle the licenses on your selected nodes.

- a. Select the Schedule recycling checkbox.



- b. Create a daily, weekly, or monthly license recycling schedule.

For **daily license recycling**, click the drop-down menus and select the occurrence and date values, and then select the starting date.

For example, every 60 minutes starting on April 17th at 5 PM...

Every
60
Minutes

Starting
17 Apr 2024
5:00 PM
Etc/UTC

Occurrence: every 60 minutes starting on 2024-04-17 at 5:00 PM Etc/UTC

...every eight hours starting on April 17th at 5 PM...

Every
8
Hours

Starting
17 Apr 2024
5:00 PM
Etc/UTC

Occurrence: every 8 hours starting on 2024-04-17 at 5:00 PM Etc/UTC

...or every seven days starting on April 17th at 5 PM.

Every
^
v
Days
v

At time
🕒
Etc/UTC

Starting
📅

Occurrence: every 7 days at 5:00 PM Etc/UTC starting on 2024-04-17

For **weekly license recycling**, select Weekly and the weekly occurrence in the drop-down menus and checkboxes.

For example, every week on Monday and Friday starting on April 17th at 5 PM.

Every
^
v
Week
v

On the
☒ Mon
☐ Tue
☐ Wed
☐ Thu
☒ Fri
☐ Sat
☐ Sun

At time
🕒
Etc/UTC

Starting
📅

Occurrence: every week on Monday and Friday at 5:00 PM Etc/UTC starting on 2024-04-17

For **monthly license recycling**, select Month, the monthly occurrence, the day of the month, and the starting time and date.

For example, every month on the 15th day of the month starting at 5 PM on April 17th.

Every
^
v
Month
v

On the
v
day of month

At time
🕒
Etc/UTC

Starting
📅

Occurrence: every month on the 15th day of the month at 5:00 PM Etc/UTC starting on 2024-04-17

c. Click Save.

Configure the settings and services

This section describes how to configure SEM to interact with the other systems and services in your IT environment.

 See [Configure SEM to collect event data from systems and devices](#) to learn how to configure SEM to receive log events from other systems and services in your IT environment.

About the console settings

On the SEM console toolbar, click the Settings button  to access select authentication and configuration settings. The following table describes the available settings.

Tab	Settings
Authentication	Enable the local user and single sign on (SSO) authentication settings, set the minimum password restrictions for local SEM user accounts, create an LDAP configuration, and create an SSO configuration.
Events Limits	Set the live and historical event limits for each search query, as well as the maximum number of events appearing in each Events viewer filter and dashboard widget. You can enter between 100 and 10000000 (ten million). The default value is 100.
Improvement Program	Enter your email address to send usage statistics to SolarWinds to help us improve our products.
Log Forwarding	Enable log forwarding to direct your raw (unnormalized) log messages to a dedicated server. This option allows you to forward log data to third-party systems and other SIEM tools.
Manage License	View, upgrade, activate, and deactivate your SEM license.
System Resources	View the system resources , which include the platform name, memory and CPU information, and the manager name, version, and IP address. Also includes the one-click download debugs feature.
Threat Intelligence	Enable the Threat Intelligence feed , which enables SEM to detect threats based on lists of known malicious IP addresses. See Using the Threat Intelligence feed in SEM for details.

Tab	Settings
Updates	Enable automatic updates for agents and connectors .
Web Console	Create a customized plain-text notification log banner to provide information to users before they access the SEM Console.
Security	Enable the SEM security settings . Configure the subject alternative name (SAN) for the IP address or FQDN/hostname in the SEM Console. The SAN name enables the SEM Manager to detect the SEM agent properly and issue a certificate.
Sharing	Create a secure file transfer protocol (SFTP) connection to an external Microsoft Windows server to share generated SEM reports. This connection ensures that you can deliver reports that exceed your Microsoft Exchange Server attachment size limits to one or more Windows servers in your organization. This option also helps to minimize hard drive space in your SEM deployment. You can also set the maximum size limit for an email attachment containing a SEM report.

Start and stop the SEM appliance and agent

This section describe how to stop or restart the SEM appliance and the SEM Agent on Windows.

Stop or restart the SEM appliance

The following steps also apply to the SEM VM.

 Do not right-click the host and choose power off or shutdown guest. You can corrupt the SEM database and file system if you do not shut down SEM properly.

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for instructions.

2. Type `appliance` at the `cmc>` prompt.

3. Either:

- Shut down the VM:
 - a. At the `cmc::appliance>` prompt, type `shutdown`.
 - b. Follow the commands to shut down the SEM VM.

- Restart the VM:
 - a. At the `cmc::appliance>` prompt, type `reboot`.
 - b. Follow the commands to restart the SEM VM.

Stop or start the SEM Agent on Windows

1. Press the Windows key + R to open the Run dialog box.
2. Type `services.msc`, and then press Enter.

The Services window opens.
3. Scroll down and select SolarWinds Security Event Manager Agent.
4. To stop or start the service, click the Stop or Start buttons near the top of the window.

Enable log forwarding

On the SEM Console Settings page, [enable log forwarding](#) to direct your raw (unnormalized) log messages to a dedicated server. This option allows you to forward log data to third-party systems and other SIEM tools.

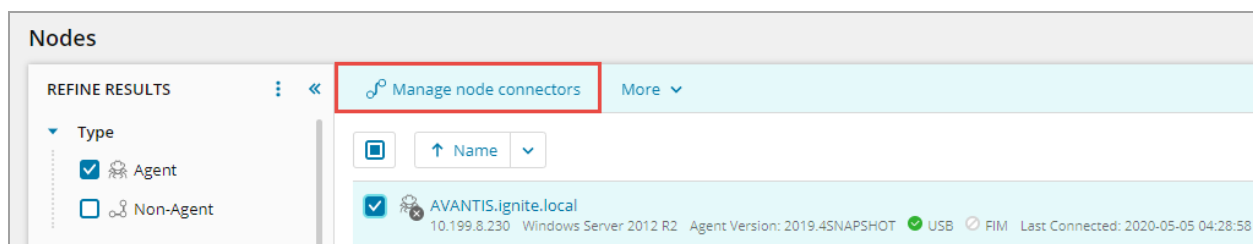
When you configure connectors to send original log data to SEM, the messages are then auto-forwarded to the designated location. To use this feature, configure the [rawlogs](#) and [applicable connectors](#) accordingly.

When enabled, you can switch between storing logs in the raw logs database and forwarding logs with syslog protocols (RFC3164 and RFC 5244). There is no option to filter logs based on IP address, connectors, rules, etc.

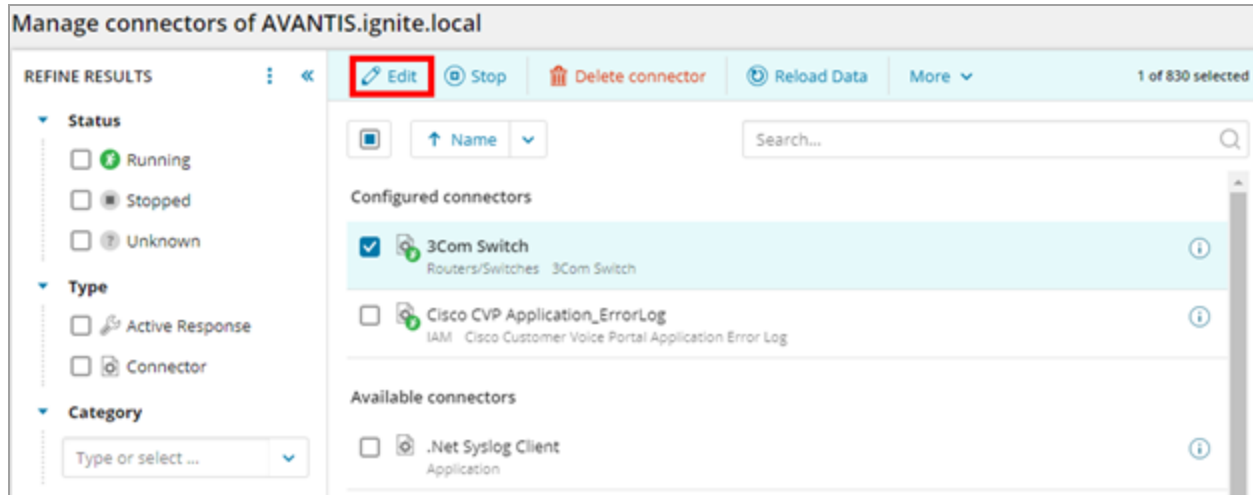
-  Rules do not fire on raw (unnormalized) log data. Rules can only fire on normalized data.
- Raw (unnormalized) log messages do not appear in Monitor view in the console.
- If you enable original log storage (raw database storage), and you enable connectors to send data to both databases, SEM storage requirements may double for the same retention period, and extra resource reservations of at least two additional CPUs and 8-16GB of RAM may be required.

Configure connectors to send original log data to SEM

1. Open the connector for editing in the Connector Configuration window for the SEM Manager or SEM Agent, as applicable:
 - **If the connector has already been configured**, stop the connector by clicking gear > Stop, and then click gear > Edit.
 - **If the connector has not been configured**, create a new instance of the connector by clicking gear > New next to the connector you want to configure.
1. On the SEM Console, navigate to Configure > Node.
2. Select an agent node, and then click Manage node connectors.



3. Select a node connector, click Stop, and then click Edit.



- Under Output, select Raw or Raw + Normalized.

Edit connector - 3Com Switch

Wrapper Name and Number

3comswitch: #27 rev.

Name

3Com Switch

Connector name

Log File

/var/log/local6.log

Directory or path to read from

Output

☐ Normalized
☒ Raw + Normalized
☐ Raw

Reader output

Sleep Time

1

Number of seconds between log reads

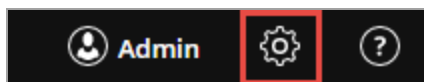
Cancel

Save

- Click Save, and then click Start.

Establish log forwarding settings

- On the SEM Console, click the Settings button.



2. On the Settings page, click the Log Forwarding tab.

AUTHENTICATION EVENTS LIMITS IMPROVEMENT PROGRAM LOG FORWARDING MANAGE LICENSE SECURITY SYSTEM RESOURCES THREAT INTELLIGENCE UPDATES	Log forwarding ☐ Enable log forwarding for adjusted connectors i Destination IP or hostname Destination port 192.168.1.1 514 ^ v Protocol UDP v RFC message format Don't know which RFC format to use? Learn more ☒ RFC 3164 ☐ RFC 5424 Severity Notice v Facility local use 0 (local0) v App name (optional) SolarwindsSEM Save Reset

3. To enable log forwarding for adjusted connectors, select the Enable log forwarding for adjusted connectors check box.



Log Forwarding can only be enabled for connectors whose Output setting includes raw logs.

4. Enter the destination IP address or host name, and then enter the destination port.
5. Select from each of the following drop-down lists (the standard settings appear by default):
 - Protocol: UDP or TCP
 - RFC format: [3164 or 5424](#)
 - Severity: The severity level is applied to all forwarded logs
 - Facility: The destination application
6. Enter an App name (optional), and then click Save.
7. To return to the SEM Console, click the Events tab.

Manage the SEM licenses

View SEM license information

Use the following steps to view SEM license information.

 See [License your SEM deployment](#) in the SEM Installation and Upgrade Guide to learn how SEM is licensed.

Manage licenses

You can view your license information in the Settings window. To access, click the System icon  in the toolbar and then select Manage License.

In the Manage license window, you can view, upgrade, activate, and deactivate your SEM license. If you do not have a license or your license is inactive, Activate license is displayed in the window. Only administrators can upgrade, activate, and deactivate a license.

 The System icon  may vary depending on whether your license is active or inactive.

Settings

AUTHENTICATION	MANAGE	RECYCLE
EVENTS LIMITS	License type:	Evaluation Activate license
IMPROVEMENT PROGRAM	Maintenance license expiration:	(20 days left)
LOG FORWARDING	Total nodes:	15500
LICENSE	Used universal licenses:	803 / 7500
SYSTEM RESOURCES	Used workstation licenses:	0 / 0
THREAT INTELLIGENCE	License key:	N/A
UPDATES	Name:	visual tester
WEB CONSOLE	Email:	visual.testers@email.com
SECURITY	Phone:	777555333
SHARING		

If you do not have a license key, click Purchase license key. SEM directs you to the available licensing options located on the SolarWinds website.

See [SEM license activation](#) to activate your license online or offline.

See [Update the SEM license](#) to update your license.

After you activate your license, the Manage license window displays your license information with options to upgrade or deactivate your license.

License type:	Security Event Manager SWE8000 for SEM7500	Upgrade license Deactivate
Maintenance license expiration:	(204 days left)	
Total nodes:	15500	
Used universal licenses:	803 / 7500	
Used workstation licenses:	247 / 8000	
License key:		
Name:	visual tester	
Email:	visual.testers@email.com	
Phone:	777555333	

Download the debug logs

SEM simplifies the system troubleshooting process by adding a one-click debug log download feature, which no longer requires a third-party application and additional configuration steps.

1. On the SEM Console, click the Settings button.



2. On the Settings page, select the System Resources tab, and then click Download Debug logs.

The debug logs (.tgz file) will download to your system.

Set the date, time, and time zone on your SEM VM

This topic describes how to synchronize the date and time settings on the hypervisor and the SEM VM.

The SEM VM is configured to synchronize with the hypervisor date and time by default. If the time is off by more than five minutes, the SEM rules will not operate properly.

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for instructions.

2. Update the time zone in your SEM Manager.

- a. At the `cmc>` prompt, type `appliance`, and then press Enter.
- b. At the `cmc::appliance>` prompt, type `dateconfig`, and then press Enter.
- c. Press Enter, and then enter the current date in month/day/year format (MM/DD/YYYY).
- d. At the `cmc::appliance>` prompt, type `tzconfig`, and then press Enter.
- e. At the `Geographic area` prompt, enter the number that matches the geographical area where you live, and then press Enter.
- f. At the `Time zone` prompt, enter the name or number of the city or region that matches your time zone, and then press Enter.

 Your entry is case sensitive. Be sure to enter the city or region name correctly.

- g. At the `cmc::appliance>` prompt, type `exit`, and then press Enter to return to the main menu.

3. Update the time in your hypervisor.

- a. At the `cmc>` prompt, type `manager`, and then press Enter.
- b. At the `cmc::manager>` prompt, type `viewsysinfo`, and then press Enter.

The system information info displays.

```
Virtualization Platform: VMware
-----
Clock
  Synchronization : Enabled
  Hypervisor Time : 6 May 2016 09:07:31
  Guest Time      : Fri May 6 09:07:31 2016
```

- c. Using the keyboard, scroll down to Hypervisor Time and change the date and time so they match the date and time in the SEM Manager.

 Press `h` for help with moving and line editing commands.

- d. Using the keyboard, scroll down to Guest Time and ensure that the date and time matches the same settings in the SEM appliance.

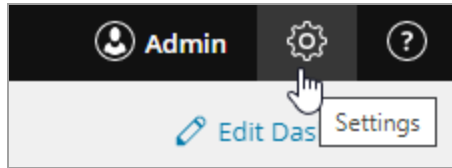
4. Type `Exit`, and then press Enter.

5. To exit the CMC interface, type `Exit`, and then press Enter again.

Configure LDAP for SEM

In SEM 2020.4 and newer versions, you can create multiple LDAP connections.

1. Click the settings icon on the upper right.



2. Select Authentication > LDAP Configuration.

AUTHENTICATION	LOGIN OPTIONS	LOCAL USERS	LDAP CONFIGURATION	SSO CONFIGURATION
EVENTS LIMITS	LOCAL USERS			
IMPROVEMENT PROGRAM	Local users authentication allows users created in SEM appliance to log into web UI and SEM Reports with set credentials. This option can only be turned off if there is a proper LDAP configuration created. Learn more			
LOG FORWARDING	☒ Allow local users authentication			

If any LDAP configurations have already been created these are displayed.

AUTHENTICATION	LOGIN OPTIONS	LOCAL USERS	LDAP CONFIGURATION	SSO CONFIGURATION
EVENTS LIMITS	+ Create configuration 🔄 Reload data			
IMPROVEMENT PROGRAM	↑ Name ↓ Search...			
LOG FORWARDING	☒ Directory Service Query Tool aadvra.local Server: 10.199.78.89 Domain: aadvra.local ⋮			
MANAGE LICENSE	☒ YURII.local Server: 10.199.76.66 Domain: YURII.local SSL ⋮			
SECURITY	☒ dh.local Server: 10.199.76.139 Domain: dh.local SSL Authentication ⋮			
SYSTEM RESOURCES	☒ ignite Server: 10.199.8.30 Domain: IGNITE.LOCAL SSL ⋮			
THREAT INTELLIGENCE				

3. Click Create configuration.

The Create LDAP Configuration dialog is displayed.

Create LDAP Configuration

×

Configure LDAP

Confirm Certificate

Summary

Configure LDAP

Configuration Name

ⓘ

This is required

IP or Hostname

Domain

Directory Service Server User Name

Directory Service Server Password

✓

Use SSL Encryption

LDAP Port

Cancel

Next >

4. Enter the following information:

Field	Description
Configuration Name	Enter a friendly name of your choosing for the LDAP configuration.
IP or Hostname	Enter the IP address or host name of your LDAP server.
Domain	Enter the fully-qualified domain name for the account store.
Directory Service Server User Name	Use the format account_name@example.com. SolarWinds recommends using a Directory Service account to prevent integration issues if the software license expires. The user name does not require special privileges (such as Domain Admin) to be a Directory Service user.
Directory Service Server Password	Enter the password for the user account.
Use SSL Encryption	(Optional) Select to use the transport layer security protocol (LDAPS) for a secure connection. This option directs traffic from the SEM VM to a designated server (usually a domain controller) for use with the Directory Service tool.
LDAP Port	If SSL encryption is not used, the default for this setting is 389. If SSL encryption is used, the default for the port is 636.
Use for Authentication	Select, then click Next if you wish to use Advanced Settings shown below.
Domain Aliases (Optional)	Specify any Domain Alias names that should be authenticated using this LDAP configuration. (The role/group names configured on this page will also apply.)
NetBIOS Names (Optional)	Specify any NetBIOS names that should be authenticated using this LDAP configuration. (The role/group names configured on this page will also apply.)
Admin Group (Optional)	Specify the DS group in Active Directory to use for the SEM administrator role. If you do not specify a name, the default ROLE_LEM_ADMINISTRATORS group is used.

Field	Description
Alerts Only Group (Optional)	Specify the DS group in Active Directory to use for the SEM auditor role. If you do not specify a name, the default ROLE_LEM_AUDITOR group is used.
Guest Group (Optional)	Specify the DS group in Active Directory to use for the SEM guest role. If you do not specify a name, the default ROLE_LEM_GUESTS group is used.
Notify Only Group (Optional)	Specify the DS group in Active Directory to use for the SEM notifications role. If you do not specify a name, the default ROLE_LEM_CONTACTS group is used.
Reports Group (Optional)	Specify the DS group in Active Directory to use for the SEM reports role. If you do not specify a name, the default ROLE_LEM_REPORTS group is used.

- Click Next.
- If you are using SSL encryption, the SSL certificate will be shown. Click I trust this certificate to confirm.
- Click Finish to create this configuration.
- Configurations can be sorted by name. For each configuration, the name, server, and domain are displayed, plus flags to show if they use SSL and/or used for Authentication.

Enable and disable LDAP configurations

Configurations are enabled as soon as they are created.

Use the toggles to disable or enable individual LDAP configurations.

 A warning message is displayed if you disable a configuration informing you that users will be unable to log on from that domain and any logged-in users from that domain will be immediately logged out.

Edit or delete an LDAP configuration

- To edit or delete an LDAP configuration, click on the vertical ellipsis icon after the configuration.



- Click Edit to display the Configure LDAP details for this configuration (which can now be saved) or click Delete to remove this configuration.

Configure the Email Active Response connector

Configure the Email Active Response connector in SEM to send automated emails to console users when a rule is triggered. This connector specifies the SMTP Relay mail host used to send emails and provides the requisite server credentials.

i If you used the SEM Setup Wizard during the installation procedure to set up your SEM environment, the Email Active Response connector is already configured.

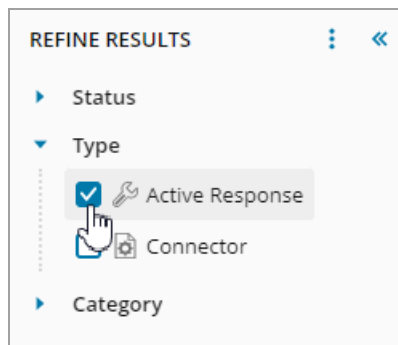
Requirements

- An email server that allows SEM to relay email messages through it
- IP address or hostname of your email server
- A return email address for bounced messages and replies
- User credentials for your email server, only if your email server requires internal users to authenticate to send email

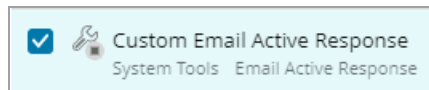
i To configure SEM to use Office 365 as a mail host, see [Configure SEM to send email via Office 365](#) in the SolarWinds Success Center.

Configure the Email Active Response connector

1. Log in to the SEM Console as an administrator.
2. On the toolbar, click Configure > Manager connectors.
3. In the Refine Results column, maximize Type and select Connector to refine the connector list to active response connectors.



4. Select an active response connector in the list. For example:

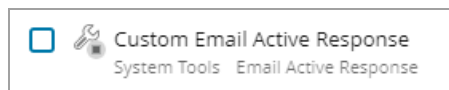


Click  to view a description of the connector.

5. Click Stop.



The green indicator next to the connector name disappears, indicating that the connector is stopped.



6. Reselect the targeted connector, and then click Edit in the toolbar.



7. Edit the node connector profile as required.

- In the Name field, enter a new name or keep the existing name.

Name
Custom Email Active Response
Connector name

- In the Mail Host field, verify that the IP address or hostname is correct.

Mail Host
example.com

If you use a hostname (as shown above), SEM Manager must be able to resolve the mail host from the DNS entries you entered when you configured your SEM network.

- In the Transport Protocol field, verify that the selected protocol is correct. To update, click the drop-down arrow and select SMTP, SSL, or TLS.

Transport Protocol
SMTP

In this example, SMTP is selected as the transport protocol.

 TLS 1.2 is supported for email connections in SEM 2020.2.1 and later.

- d. Verify that the port value is correct.

Port
25

Based on the value you selected in the Transport Protocol field, this field defaults to one of the following ports:

- 25 (Standard, non-encrypted SMTP)
- 465 (SSL with encryption)
- 587 (TLS with encryption)

- e. In the Return Address field, verify that the return address is correct. Edit if required. For example:

Return Address
noreply@solarwinds.com

 This field is pre-populated with noreply@solarwinds.com. Be sure to change this email address to an address associated with your organization.

- f. In the Return Display Name field, verify that the return display name is correct. Edit if required. For example:

Return Display Name
SolarWinds

- g. (Optional) If the email server requires an Active Directory user to send email, enter the authentication server user name in the Authentication Server Username field.

Authentication Server Username
admin

- h. (Optional) If the email server requires an Active Directory user to send email, ensure that an authentication server password exists in the Authentication Server Password field.

Authentication Server Password

 If you are retesting the email configuration, re-enter the password.

- i. (Optional) In the Test E-mail Address field, verify that the e-mail address is correct. This address is used to verify that an e-mail can be sent to a user when generated by an active response connector. For example:

Test E-mail Address
user@example.com

 If the email server requires an email to be sent from a computer within the domain, the email server must have an exception created for the SEM hostname. SEM cannot join the domain.

- j. (Optional) Click Test Email to test.

Test Email

If the test message was sent successfully through the SMTP server, the following message displays in the console:

 Success The test message has been sent using the provided mail server. Please check your mailbox.	

If the test message was not sent successfully through the SMTP server, a message displays in the console. For example:

 Error Failed to connect to the server. Please check the Mail Host, Port, and Protocol fields.	

The Error test message provides details about the failure and provides suggestions to troubleshoot the failure.

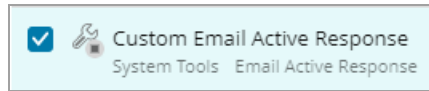
 The response message may require up to 30 seconds to display in the console. If you do not receive a response, the e-mail address in the Test E-mail Address field may be incorrect or SEM cannot reach the SMTP server through your network.

- k. (Optional) Verify that the user who owns the test e-mail address received the test email.

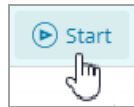
I. Click Save.

Your changes are saved to the connector profile.

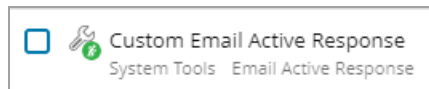
8. Make sure the connector checkbox is selected.



9. Click Start.



The green indicator next to the connector name displays, indicating that the connector is started and running.



Test the Email Active Response connector

Send a test email to verify that the connector is working properly.

If you receive an email, the connector is working properly. If you do not receive an email, the SEM Internal Events filter provides the following information:

- Event Name: InternalInfo
- Event Info: Email notification failed
- Extraneous Info: Information about the failure. For example, server not reachable, authentication issue, and so on.

Modify the connector configuration as required and then resend a test email.

Enable SEM to receive SNMP traps

Turn on the SNMP Trap Logging Service to enable SEM to receive SNMP traps from devices and applications on your network. SEM can correlate events sent as SNMP traps from devices that have a device-specific connector.

SEM can also correlate performance alerts sent as SNMP traps from the following SolarWinds solutions:

- Network Performance Monitor (NPM)
- Server & Application Monitor (SAM)
- Virtualization Manager (VMAN)

The SNMP Trap Logging Service must be enabled to correlate events sent by these SolarWinds products.

SEM receives SNMP traps on port 162.

See also:

- To configure SEM to output SNMP traps, turn on the SNMP Request Service see [Send SNMP traps from SEM to other applications](#).
- To configure SEM to communicate with NPM and the Orion Web Console, see [Monitor SEM from NPM and the Orion Web Console using SNMP](#).

Complete the following steps to enable (or disable) the SNMP Trap Logging Service in SEM.

Enable or disable the SEM SNMP Trap Logging Service

1. Open the CMC command line.

See [About the CMC command line](#) for instructions.

2. At the `cmc>` prompt type:

```
service
```

3. At the `cmc::service>` prompt type:

```
snmp
```

A prompt like the following appears:

```
SNMP Trap Logging Service is DISABLED
```

```
Would you like to ENABLE the SNMP Trap Logging Service? [Y/n]
```

If the service is running, the prompt displays:

```
SNMP Trap Logging Service is RUNNING
```

```
Would you like to STOP the SNMP Trap Logging Service? [Y/n]
```

4. Type `Y` or `n`, and then press Enter.

The SNMP Trap Logging Service is configured.

5. Next, a prompt like the following appears:

```
SNMP Request Service is DISABLED
```

```
Would you like to ENABLE the SNMP Request Service? [Y/n]
```

 The SNMP Request Service is not the same as the SNMP Trap Logging Service:

- The SEM SNMP Request Service sends SNMP traps outside of SEM
- The SEM SNMP Trap Logging Service receives SNMP traps from other devices.

Type `Y` or `n`, and then press Enter.

- If you enabled the SNMP Trap Logging Service, the following message appears:

```
The SNMP Trap Logging Service is started.
```

- If you disabled the SNMP Trap Logging Service, the following message appears:

```
The SNMP Trap Logging Service is stopped.
```

6. At the `cmc::service>` prompt, type `exit`.
7. To log out and close the CMC command-line, type `exit` again.

Monitor your SNMP traps messages in the [SEM Console](#).

Send SNMP traps from SEM to other applications

Turn on the SNMP Request Service to allow SEM to output SNMP traps to one or more applications on your network. SEM supports SNMP version 2 and SNMP version 3.

The SNMP Request Service must be turned on in SEM to do the following:

- Send SNMP traps to devices when SEM rules fire
- Use NPM and the SolarWinds Orion Web Console to monitor SEM system resources such as CPU and memory

-  If you use SolarWinds Network Performance Monitor (NPM) in your environment:
1. Enable the SNMP Request Service using the steps on this page.
 2. To set up the Orion Console for SNMP monitoring, see [Monitor SEM from NPM and the Orion Web Console using SNMP](#).

To enable or disable the SNMP Request Service

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for instructions.

2. At the `cmc>` prompt, type:

```
service
```

3. At the `cmc::service>` prompt type:

```
snmp
```

A prompt like the following appears:

```
SNMP Trap Logging Service is DISABLED
Would you like to ENABLE the SNMP Trap Logging Service? [Y/n]
```

The SNMP Trap Logging Service is not the same as the SNMP Request Service. The SEM SNMP Trap Logging Service receives SNMP traps from other devices, whereas the SEM SNMP Request Service outputs SNMP traps outside of SEM. See [Enable SEM to receive SNMP traps](#) for more information.

4. Do not change the status of this service unless you know what you are doing.

To go to the next step, type `Y` or `n`, and then press Enter.

A prompt like the following appears:

```
SNMP Request Service is DISABLED
Would you like to ENABLE the SNMP Request Service? [Y/n]
```

5. To enable or disable the service, type `Y` or `n`, and then press Enter.

If you enabled the SNMP Request Service, the following prompt appears:

```
Enter the port number to access SNMP on SEM (default: 161):
```

6. Type the port number that SEM should use to communicate with SolarWinds Network Performance Monitor (NPM), and then press Enter.

 Ports 161 and 162 are standard.

The following prompt appears:

```
Enter the username to access SNMP on SEM (default: orion):
```

7. Type the user name to use, and then press Enter.

The following prompt appears:

```
Enter the password hashing algorithm (SHA1, MD5 or NO for no
authentication, default: SHA1):
```

8. Enter an option, and then press Enter.

The following prompt appears:

```
Enter the authentication password (default: orion123):
```

9. Type the password, and then press Enter.

The following prompt appears:

```
Enter the communication encryption algorithm (AES128, DES56 or NO for no
encryption, default: AES128):
```

10. Enter an option, and then press Enter.

The following prompt appears:

```
Enter the encryption key (default: orion123):
```

11. Type the encryption key, and then press Enter.

The SNMP Request Service is started.

12. To return to the main menu, type `exit` at the `cmc::service>` prompt.

13. To log out and close the CMC command-line, type `exit` again.

Collect Windows Filtering Platform (WFP) events

Windows Filtering Platform (WFP) logs firewall and IPsec related events to the System Security log. These alerts are background events that require additional SEM resources to process and are not recommended for an optimized SEM deployment.

About Windows WFP events and SEM performance

By default, WFP logging is disabled in the Windows Security Log connector. Tuning out Windows noise in group policies has the following advantages:

- Reduces the space that these events occupy in the Security Event log
- Reduces network activity
- Reduces demand on SEM system resources (such as CPU, memory, and disk space)

 The Windows Security Log connector stopped collecting WFP data in SEM version 6.2.

Configure SEM to collect WFP events (Optional)

If necessary, you can enable WFP event logging in SEM.

 SolarWinds strongly recommends that you keep WFP logging turned off.

To collect WFP events in SEM, configure the Windows Filtering Platform Events connector. Enabling this connector will result in SEM collecting a huge volume of data. To manage this data, see the following sections.

Improve SEM performance by tuning Windows WFP events

If you collect WFP events in SEM, SolarWinds recommends tuning WFP in your Active Directory group policies to decrease the load that background events place on the SEM Manager. The following tables describe alerts located in the Event Distribution Policy in SEM Manager. You can filter out these events by clearing the appropriate check boxes in the Console, Database, Warehouse, and Rules columns. SEM will process the remaining events.

 In SEM, the terms *event* and *alert* are interchangeable.

SolarWinds recommends disabling WFP alerts using Group or Local Policy.

 The ProviderSID value in the following alerts match the `Windows Security Auditing Event ID` format where *Event ID* is one of the Windows Event IDs listed in the following table.

Alert Name	Windows Event ID
TCPTrafficAudit	5152, 5154, 5156, 5157, 5158, 5159
IPTrafficAudit	5152, 5154, 5156, 5157, 5158, 5159
UDPTrafficAudit	5152, 5154, 5156, 5157, 5158, 5159
ICMPTrafficAudit	5152, 5156, 5157, 5158, 5159
RoutingTrafficAudit	5152, 5156
PPTPTrafficAudit	5152

Table of Descriptions by Event ID

Event ID	Brief Description
5152	Windows Filtering Platform blocked a packet
5154	Windows Filtering Platform permitted an application or service to listen on a port for incoming connections
5156	Windows Filtering Platform allowed a connection
5157	Windows Filtering Platform blocked a connection
5158	Windows Filtering Platform permitted a bind to a local port
5159	Windows Filtering Platform blocked a bind to a local port

Monitor SEM from NPM and the Orion Web Console using SNMP

If you use Network Performance Monitor (NPM) and the SolarWinds Orion Web Console, you can use it to monitor CPU, memory, and other critical resources utilized by SEM. Complete the steps in this topic to configure SEM to communicate with NPM.

 SEM can use SNMP version 3 to communicate with SolarWinds Network Performance Monitor (NPM).

Enable the SNMP Request Service

See [Provide SNMP traps from SEM to other applications](#) for details. After you enable and configure the SNMP Request Service, go to the next topic, Set up the Orion Web Console for SNMP monitoring.

Set up the Orion Web Console for SNMP monitoring

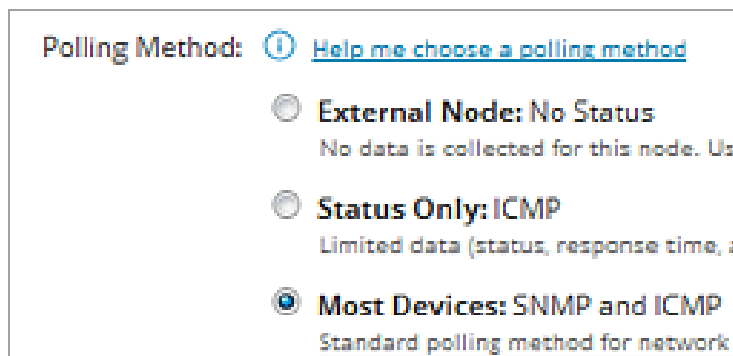
When you are finished enabling the SNMP Request Service, log in to the Orion Web Console and set up the SEM Manager as a monitored node on the Orion Platform.

1. Log in to your Orion Web Console as an administrator.
2. Navigate to Settings > Manage Nodes, and then click Add a Node.

If the node already exists and it is not managed, click the node and select Not Managed Node > Yes to manage the node.

The Define Node dialog displays.

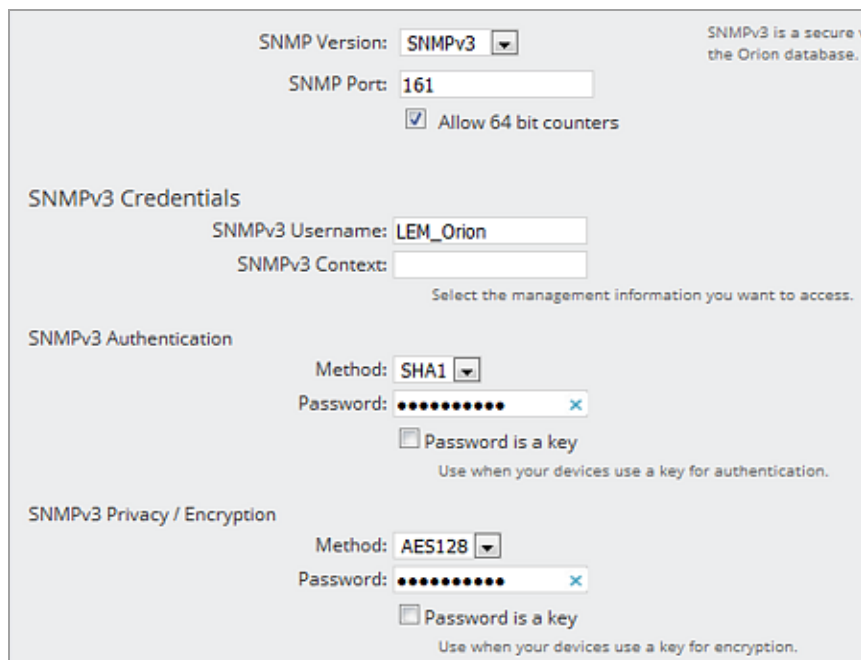
3. In the Polling Hostname or IP Address field, enter the IP address of the SEM Manager.
4. Under Polling Method, select Most Devices: SNMP and ICMP.



Polling Method: [Help me choose a polling method](#)

- ☐ **External Node: No Status**
No data is collected for this node. Use only for monitoring.
- ☐ **Status Only: ICMP**
Limited data (status, response time, and latency).
- ☒ **Most Devices: SNMP and ICMP**
Standard polling method for network devices.

5. Select your polling method settings.



SNMP Version: **SNMPv3** SNMPv3 is a secure version of the Orion database.

SNMP Port: **161**

☒ Allow 64 bit counters

SNMPv3 Credentials

SNMPv3 Username: **LEM_Orion**

SNMPv3 Context:

Select the management information you want to access.

SNMPv3 Authentication

Method: **SHA1**

Password:

☐ Password is a key
Use when your devices use a key for authentication.

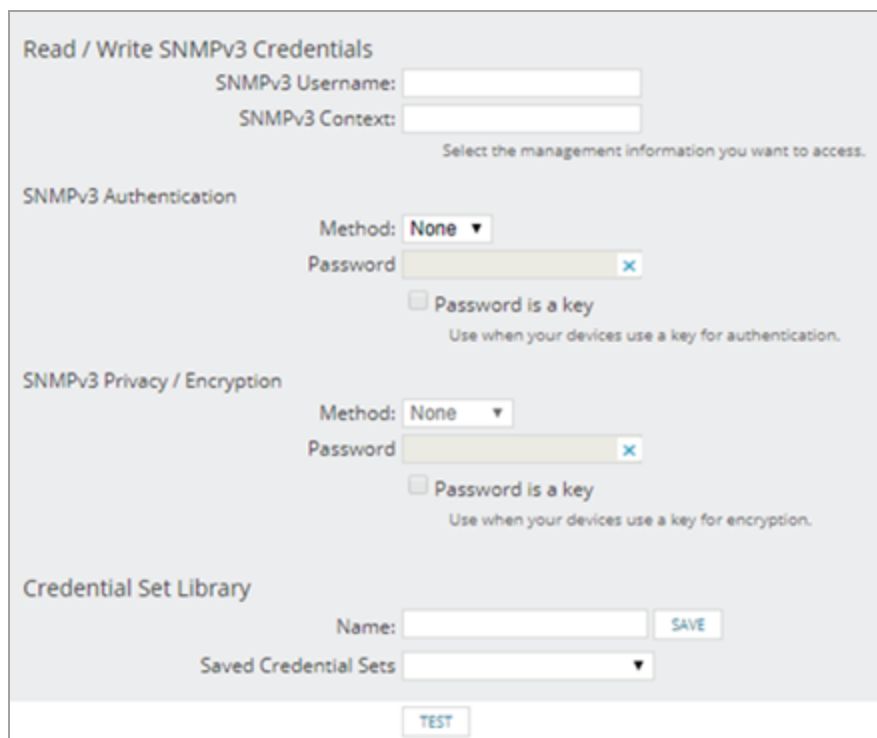
SNMPv3 Privacy / Encryption

Method: **AES128**

Password:

☐ Password is a key
Use when your devices use a key for encryption.

- a. From the SNMP drop-down list, select SNMPv3.
 - b. Enter the port number used to access SNMP on the SEM appliance.
 - c. Under SNMPv3 Credentials, enter the user name used to access SNMP on the SEM appliance.
 - d. Under SNMPv3 Authentication, enter the hashing algorithm method and password.
 - e. Under SNMPv3 Privacy / Encryption, enter the communication encryption algorithm and password.
 - f. Accept the default selections in the remaining options.
6. In the lower section of the form, ensure the fields remain blank.



 This is a SEM-specific setting for SNMPv3. Completing the Username and Context fields, for example, will cause the connection test to fail.

7. To test the connection, click Test.

If the connection is good, Test Successful appears. If it fails, [troubleshoot your Orion connection](#).

8. Click Next.

The Orion Platform authenticates the SEM Manager and runs a discovery to locate the resources available to monitor on the SEM appliance. The discovered resources will list all the elements that are available to monitor. The Orion Platform will automatically provide a list of selected resources based on the device type.

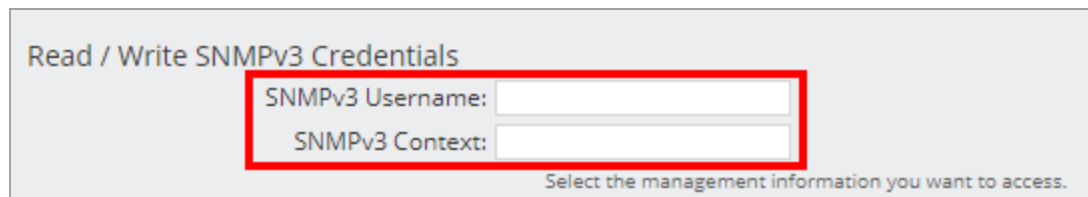
9. In the Choose Resources dialog, select the resources to monitor on the node, and then click Next.
10. In the Add Application Monitors dialog, click Next.
11. In the Change Properties dialog, click Next.
12. Click OK, Add Node.

The SEM appliance is added to the Orion Web Console for monitoring.

Troubleshooting your Orion connection

If you cannot establish a connection between your SEM appliance and the Orion Platform:

- Ensure that the settings you entered in the Define Node window match the settings used to enable the SNMP Request Service.
- Review the Orion logs located at `c:\ProgramData\SolarWinds\Discovery` for errors.
- Ensure the Username and Context fields in the lower half of the polling method configuration settings are empty.



See [Unable to add nodes through the Web Console](#) for additional troubleshooting information.

Create a custom log in banner

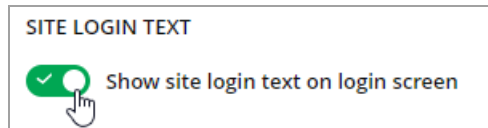
You can create a customized plain-text notification banner to provide information to users before they access the SEM Console.

 You cannot add images to this banner.

1. On the SEM Console, click the Settings button.



2. On the Settings page, click the Web Console tab.
3. Drag the toggle switch to the right.



4. Enter up to 3500 characters in the text box.

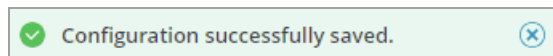
Text

Enter text here.

Maximum length is 3500 symbols.

5. Click Save.

A message displays confirming your changes.

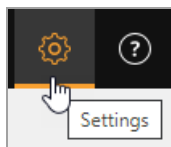


Set the maximum email attachment size

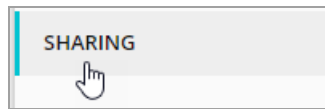
You can restrict the email attachment size to conform with your email provider restrictions. This setting will alert you when a scheduled or generated report exceeds the maximum attachment size you enter in this setting.

 If your reports exceed your email provider restrictions, consider [setting up a secure file transfer protocol \(SFTP\) connection](#) to one or more external Microsoft Windows servers. This option allows you to deliver your reports directly to selected stakeholders in your organization.

1. Log in to SEM as an administrator.
2. In the toolbar, click the Settings icon.



3. In the Settings screen left column, click Sharing.



4. Click the Email tab.
5. In the Maximum attachment size field, enter the maximum attachment size in megabytes based on your email provider restrictions. If your provider does not have any limitations, set the maximum attachment size based on your SEM deployment restrictions.

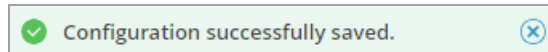
 The default size is 10 MB. You can enter 1 MB up to 10240 MB (10 GB).

For example, 2000.



6. Click Save.

A message displays confirming the new configuration.



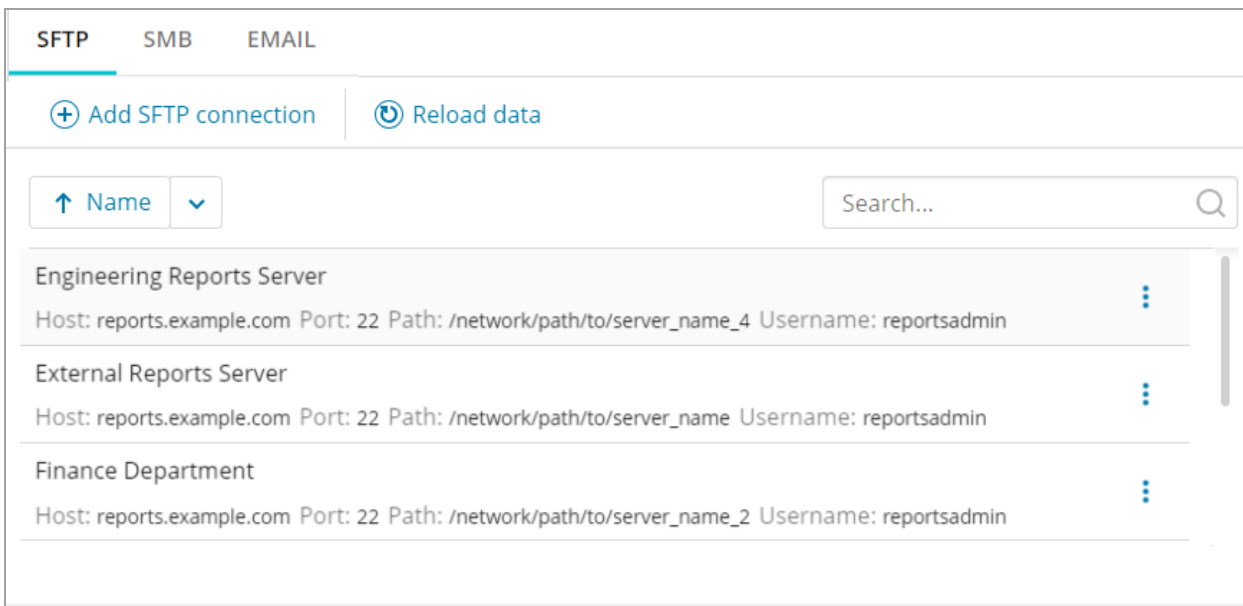
(Optional) Set up SFTP connections to external systems

You can save your SEM reports to one or more Windows or non-Windows systems using a secure file transfer protocol (SFTP) connection. This option ensures that you can deliver large reports that may exceed your email requirements to one or more systems in your organization. This option also helps to minimize hard drive space in your SEM deployment.

 SFTP uses SSH to ensure that all reports sent to an external server are secure in transit from unauthorized users.

You can set up as many SFTP connections as you need. This process helps you streamline your SEM reports delivery to department and management servers where authorized personnel can access their requested reports in a timely manner.

Below is an example of the SFTP connections screen. Each connection lists the server hostname or IP address, server port number, network path to the server, and the server username. After you [add a new SFTP connection](#), you can [edit](#), [copy](#), or [delete](#) the connection.



Locate an SFTP connection

The following table describes how to locate SFTP connections in the Settings > Sharing > SFTP tab.

Action	Description
Locate a specific connection	Enter a search term in the Search field and then click the magnifying glass  to display the results.
Display all connections by host or name	Click  in the toolbar.
List all connections in ascending or descending order	Click Name in the toolbar.
Collect the latest connection and redisplay the results	Click Reload data in the toolbar.

Set up an SFTP server

You can set up a Windows or non-Windows system as your SFTP server. The system must have the SFTP protocol enabled to establish an SFTP connection.

Set up an SFTP server using SolarWinds SFTP/SCP Server

For Windows systems, SolarWinds recommends [SolarWinds SFTP/SCP Server](#). This free tool allows you to transfer files up to 4 GB in size to a Windows system.

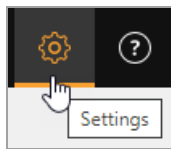
1. Select a Windows system in your organization as a dedicated SFTP server.
2. Log in to the system as an administrator.
3. Enable the SFTP protocol on the system.

 See your operating system documentation for instructions.

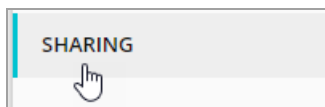
4. Navigate to the [SolarWinds SFTP/SCP Server](#) website.
5. Click Download Free Tool.
6. Complete the online form, and then click Proceed to Free Download.
7. Follow the online prompts to complete the download.
8. Run the installer on the Windows system.
9. [Add a new SFTP connection](#) to the Windows system.

Add a new SFTP connection

1. Locate a Windows or non-Windows system on your network that will store your SEM reports.
2. Verify that the SFTP protocol is enabled on:
 - The system designated as the SFTP server
 - The system hosting your SEM deployment
3. Log in to SEM as an administrator.
4. In the toolbar, click the Settings icon.



5. In the Settings screen left column, click Sharing.



6. Click the SFTP tab.
7. Click Add SFTP connection.
8. In the SFTP tab, click Add SFTP connection.
9. In the Name field, enter a name for this SFTP setting. For example:

Name

External Reports Server

10. In the Host field, enter the hostname or IP address of the target SFTP server where you want to store the reports. For example:

Host

reports.example.com

11. In the Port field, enter the port number of the target SFTP server. The default is port 22. For example:

Port

22

^
v

12. In the Username field, enter a username for this SFTP server. For example:

Username

reportsadmin

13. In the Password field, enter a user password for this connection.

Password

14. In the Path field, enter the network path to the reports server. For example:

Path

/network/path/to/server_name

15. Click Create.

Create

A message displays, confirming the new connection.

✓

Sftp configuration saved

✕

The new connection displays in the Settings menu.

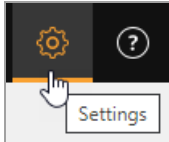
External Reports Server
⋮

Host: reports.example.com Port: 22 Path: /network/path/to/server_name Username: reportsadmin

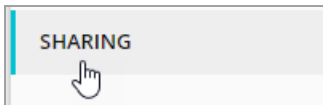
16. Repeat step 1 through step 13 to create additional SFTP connections in your organization.

Edit an SFTP connection

1. Log in to SEM as an administrator.
2. In the toolbar, click the Settings icon.



3. In the Settings screen left column, click Sharing.

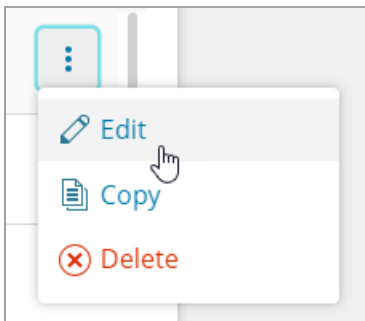


4. Click the SFTP tab.
5. Locate a connection you want to edit. For example:

External Reports Server
⋮

Host: reports.example.com Port: 22 Path: /network/path/to/server_name Username: reportsadmin

6. Click ⋮ and select Edit.



7. Edit the SFTP connection settings as required. For example, you can change the connection name.

Edit SFTP connection

Name

Finance Department

Host

reports.example.com

Port

22

^

v

Username

reportsadmin

Password

Path

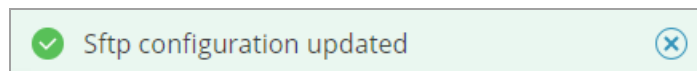
/network/path/to/server_name

Cancel

Save

8. Click Save.

A message displays, confirming the edit.



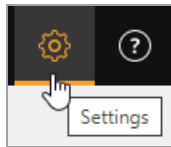
The updated connection displays in the Settings window.



Copy an SFTP connection

If you plan to create several SFTP connections in your deployment with a similar path, copy an existing connection and then change the name and path to the new external server.

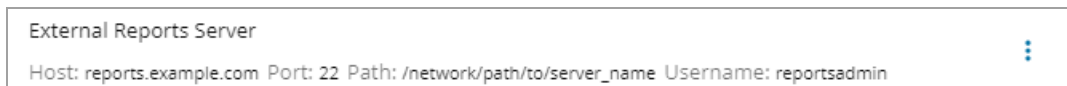
1. Log in to SEM as an administrator.
2. In the toolbar, click the Settings icon.



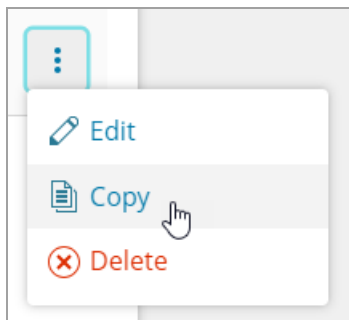
3. In the Settings screen left column, click Sharing.



4. Click the SFTP tab.
5. Locate a connection you want to copy. For example:



6. Click  and select Copy.



7. Update the connection settings with a unique name and path.

In the following example, the connection name is changed to Finance Department and the server name is changed to server_name_2.

Copy SFTP connection - External Reports Server

Name

Finance Department

Path

/network/path/to/server_name_2

Cancel

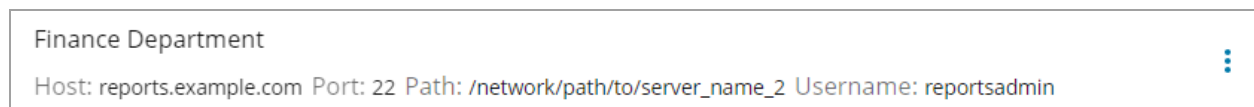
Copy

- Click Copy.

A message displays, confirming the copy.

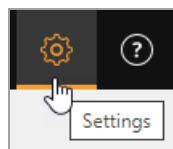


The copied connection with the new connection settings displays in the Settings window.

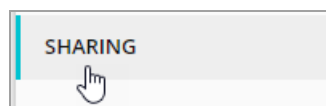


Delete an SFTP connection

- Log in to SEM as an administrator.
- In the toolbar, click the Settings icon.



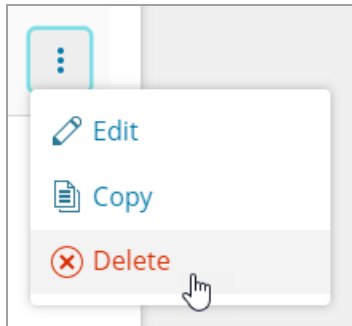
- In the Settings screen left column, click Sharing.



- Click the SFTP tab.
- Locate a connection you want to delete. For example:

External Reports Server	⋮
Host: reports.example.com Port: 22 Path: /network/path/to/server_name Username: reportsadmin	

6. Click  and select Delete.



The following message displays in the console.

 **Delete selected sftp connection?**


Deleting this sftp will result in losing current configuration.

Cancel
Delete

7. Click Delete.

The connection setting is deleted from the Settings window.

(Optional) Set up SMB file sharing to a Windows server

You can publish SEM reports to a file share an external Windows server using server message block (SMB) file sharing. This feature can help you streamline your SEM report delivery to department and management servers where authorized personnel can access their requested reports in a timely manner. You can configure SMB file sharing to one or more shares on a single Windows server.

When you [run or schedule a SEM report](#), you can select the SMB connection as a sharing option.

 SMB uses SSH to ensure that all reports sent to an external server are secure in transit from unauthorized users.

Below is an example of the SMB configuration screen. Each connection lists the network path to the Windows share, server port number, and the username of the user who created the connection. After you [create a new SMB connection](#), you can [reload](#), [edit](#), [copy](#), or [delete](#) the connection.

SFTP
SMB
EMAIL

+ Create SMB configuration
⌂ Reload data

↑ Name ↓
Search...

Marketing
Path: \\10.199.89.94\test-share Port: 445 Username: administrator

Locate an SMB connection

The following table describes how to locate SMB connections in the Settings > Sharing > SMB tab.

Action	Description
Locate a specific connection	Enter a search term in the Search field and then click the magnifying glass  to display the results.
Display all connections by host or name	Click  in the toolbar.
List all connections in ascending or descending order	Click Name in the toolbar.
Collect the latest connection and redisplay the results	Click Reload data in the toolbar.

Create an SMB configuration

[Set up a network share on a Windows server](#) and then [create a new SMB configuration](#). The Windows server must have the SMB protocol enabled to establish an SMB connection.

 You can create multiple SMB configurations on only one Windows server.

Set up a network share on a Windows server

1. Select a Windows-based system in your organization to store your SEM reports.
2. Log in to the system as an administrator.
3. Enable the SMB protocol on the system and record the SMB version. You will need this information for a future step.

 See your operating system documentation for instructions.

- On the server, open File Explorer and create a network share to store the [scheduled reports](#).

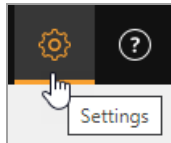
Ensure that:

- The share name does not exceed 64 characters.
- The share name does not include blank spaces.
- The path to the network share does not exceed 64 characters.

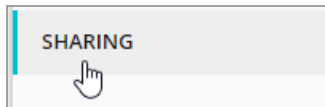
- Record the network path to the network share. You will need this information for a future step.
- Verify that the identical SMB protocol is enabled on your SEM server.

Create a new SMB configuration

- Log in to SEM as an administrator.
- In the toolbar, click the Settings icon.



- In the Settings screen left column, click Sharing.



- Click the SMB tab.



- Click Add SMB configuration.



- In the Name field, enter a name for this SMB configuration.

For example:

Name
Marketing

 You can enter a name that includes up to 64 characters.

7. In the Path field, enter the network path to the Windows share on the targeted server.

For example:

Path

Example: \\server\share

 You can enter a path that includes up to 4096 characters.

8. In the Port field, enter the port number of the target Windows server or accept the default selection. The default is port 445.

For example:

Port




9. In the Username field, enter the name of the user who has the rights to the network share on the Windows server. Ensure that the user name does not exceed 64 characters.

For example:

Username

Example: "username", "domain\username" or "username@domain"

10. In the Password field, enter the password of the user who has the rights to the network share.

Password

11. Click the Minimum SMB version drop-down arrow and select the SMB version (for example, SMB311) that is running on the server hosting the network share.

For example:

Minimum SMB version



12. Click Test.

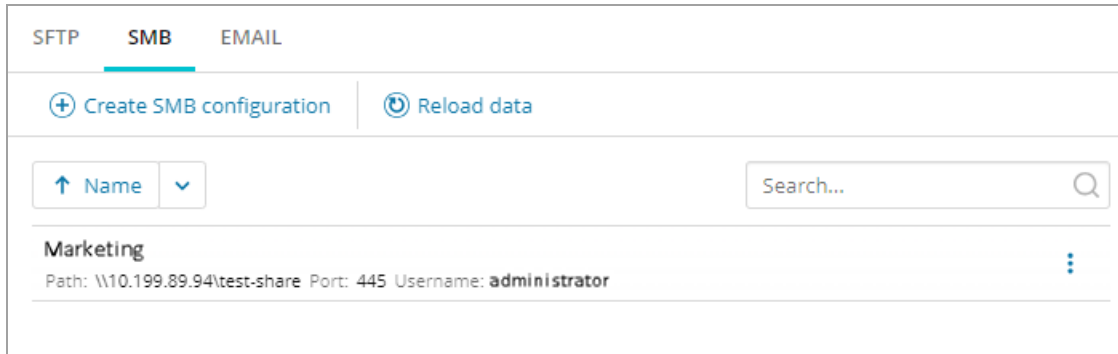


If the username and password are valid, a message displays that confirms the new connection.



13. Click Create.

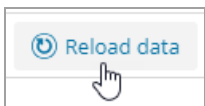
The new connection displays in the SMB window.



14. Repeat step 1 through step 13 to create additional SMB configurations to network shares in your organization.

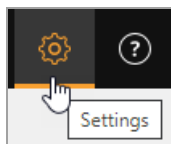
Reload the connection data

To refresh your connection data, click Reload data in the SMB tab. When completed, all SMB connections in the SMB tab will contain the latest configuration data.

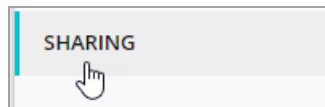


Edit an SMB connection

1. Log in to SEM as an administrator.
2. In the toolbar, click the Settings icon.



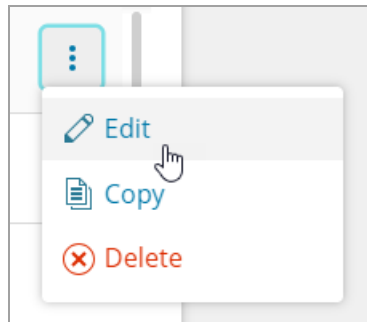
3. In the Settings screen left column, click Sharing.



4. Click the SMB tab.



5. Locate a connection you want to edit.
6. In the targeted connection, click  and select Edit.



7. Edit the SMB connection settings as required.

For example, you can change the connection name.

 Re-entering the username and password is not required.

Edit SMB configuration - Marketing

Name

Path

Port

^

v

Example: \\server\share

Username

Example: "username", "domain\username" or "username@domain"

Password

Minimum SMB version

SMB311 (Windows 10/Server 2016) v

Cancel

Test

8. Click Test.

If the username and password are valid, a message displays that confirms the new connection.



9. Click Create.

The updated connection displays in the Settings window.

SFTP **SMB** EMAIL

+ Create SMB configuration

🔄 Reload data

↑ Name

v

Search...

Finance

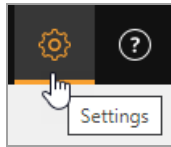
Path: \\10.199.89.94\test-share Port: 445 Username: administrator

⋮

Copy an SMB connection

If you plan to create several SMB connections in your deployment with a similar path, you can copy an existing connection and change the configuration settings and path to the new network share.

1. Log in to SEM as an administrator.
2. In the toolbar, click the Settings icon.



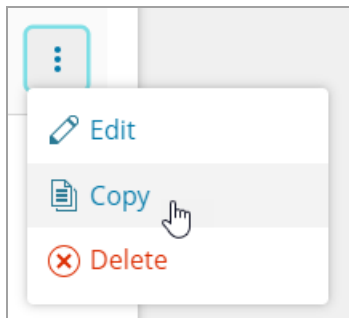
3. In the Settings screen left column, click Sharing.



4. Click the SMB tab.



5. Locate a connection you want to copy.
6. Click  and select Copy.



7. Update the connection settings with a unique name and path.

Copy SMB configuration - Marketing

Name

Copy of sdsad

Path

\\10.199.89.94\test-share

Example: \\server\share

Cancel

Test

8. Click Test

If the username and password are valid, a message displays that confirms the new connection.



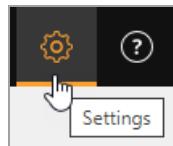
9. Click Copy.

The copied connection with the new connection settings displays in the SMB window.

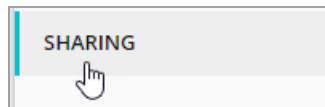
Delete an SMB connection

1. Log in to SEM as an administrator.

2. In the toolbar, click the Settings icon.



3. In the Settings screen left column, click Sharing.



4. Click the SMB tab.

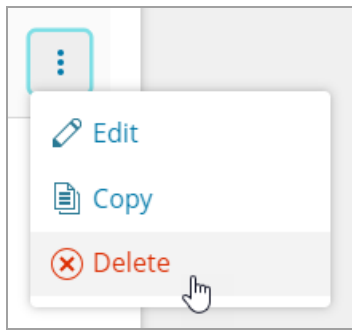


5. Locate a connection you want to delete.

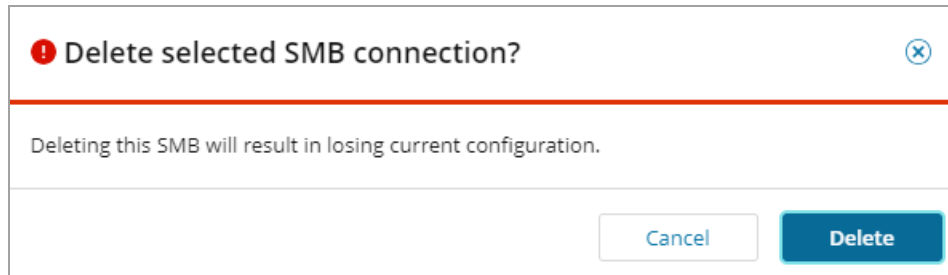
For example:



6. Click and select Delete.



The following message displays in the console.



7. Click Delete.

The connection is deleted from the Settings window.

SEM Console

The SEM Console includes a toolbar that provides additional views with details about your deployment.

These views include:

- [Dashboard](#)
- [Live Events](#)
- [Historical Events](#)
- [Rules](#)
- [Configure](#)

Dashboard

Access the SEM Dashboard to highlight and summarize trends and suspicious activity through a series of interactive widgets. You can create, edit, and arrange widgets to display log data in a variety of tables and graphs based on filters within your Events viewer. Upon initial login, the SEM Dashboard appears by default.

See [SEM Dashboard](#) for more information.

Live Events

Live Events display all live event data that is passing through a particular SEM Manager instance. Use this view to monitor real-time events as they occur in your deployment.

Within the console view, you can switch between live and historical event views based on user-defined date and time parameters. All established SEM Monitor filters are accessible on the SEM Console Filters pane.

See [Live Events view](#) for more information.

Historical Events

Historical Events provide historical record archives for in-depth analysis and troubleshooting. You can use the historical data search to conduct custom searches, investigate your search results and event data, and then act on your findings. You can create and save a search query, as well as generate reports for each query.

Within the console view, you can switch between historical and live event views based on user-defined date and time parameters. All established SEM Monitor filters are accessible on the SEM Console Filters pane.

See [Analyze Historical data](#) for more information.

Rules

Rules monitor event traffic and automatically respond to security events in real time, whether you are monitoring the console or not. When an event (or a series of events) meets a rule condition, the rule prompts the SEM manager to act. A response action can be discreet (for example, sending a notification to select users by email), or active (for example, blocking an IP address or stopping a process).

See [Create rules that respond to security events](#) for more information.

Configure

Configure provides a lists of options you can use to configure the SEM Console.

Using the Configure menu selections, you can add agent nodes, configure connectors and connector profiles, and then monitor activity on the SEM Console. After you configure the nodes and connectors, click the Events tab to view your network activity. Here, you can create and apply filters to tailor your log feed to view event logs vital to maintaining the health of your network environment.

See [Create rules that respond to security events](#) for more information.

The following table lists the options (in alphabetical order) that are available in the Configure menu.

Option	Description
Connector profiles	Displays a list of all connector profiles. You can refine the list by modification type and create a new connector profile.
Directory service groups	Displays a list of all directory service groups. You can import a directory service group, synchronize all groups, and refine the list by creator, last synchronized time, connection, and LDAP status.

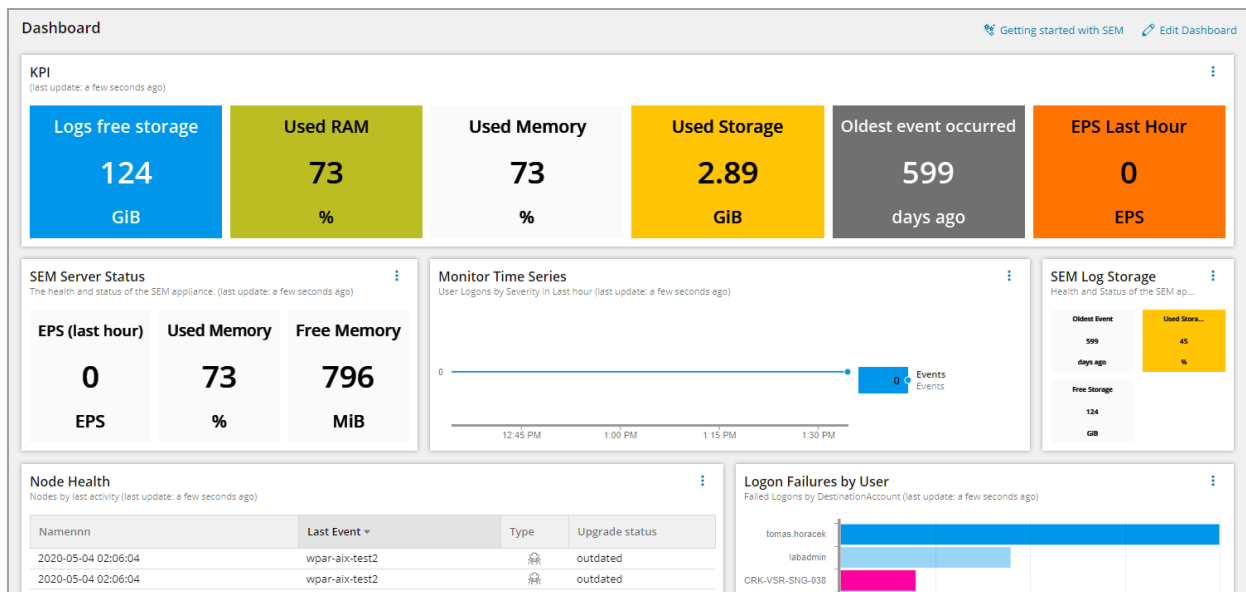
Option	Description
Email templates	Displays a list of email templates used for notifications when triggered as a response in a custom rule. You can create a new email template and refine the list by last user modification and last modification time. You can use email templates to customize your email notifications when triggered as responses in your custom rules. An email template includes static and dynamic text (or parameters). The static text lets you customize the message body of the email. The dynamic text is pulled from the original event that caused the rule to fire.
Event groups	Displays a list of all event groups used in SEM. Event groups allow you to group similar events together into a single category to initiate a specific event filter, rule, or condition. You can create and import event groups, and export the existing or refined list to a JSON file.
Manager connectors	Displays a list of all configured connectors. You can refine the list by status, type, or category.
Nodes	Displays a list of all agent nodes. You can refine the nodes list by category, add an agent node, and export a list of nodes to a CSV file.
Tags management	Displays a list of all tags used in SEM. You can add a new tag and refine the list by tag category and application.
Time of day groups	Displays groups of hours that you associate with rules and filters to execute different actions at different times of the day.
Users	Displays a list of all users configured in SEM. You can add a new user and refine the user list by type, activity, role, and the last login.
User defined groups	Displays a list of all groups created by authorized SEM users. You can create a new group and refine the list by last modification user and modification time. You can create user-defined groups to organize related elements for use with rules and filters. Groups can contain elements such as events, IP addresses, computer names, and user accounts. After you define a group, it can be referenced from multiple rules and filters.

SEM Dashboard

The SEM Dashboard allows you to visualize the network and log data in your corporate environment. Using the dashboard, you can highlight and summarize trends and suspicious activity through a series of interactive widgets. You can also create, edit, and arrange widgets to display log data in a variety of tables and graphs based on filters within your Events viewer.

Although SEM provides a library of widgets, you can create your own by using filters that you customized to monitor specific activity. If your widget includes charts, you can click a specific line, bar, or pie wedge to open the source filter. The corresponding filter opens the Events viewer, and displays the targeted filter information. The filter lists only the events that correspond with the selected chart item.

To access the SEM Dashboard, click the Dashboard tab on the console toolbar.



Click an event or data point in a widget to view associated details in the Events viewer.

Clicking the Others grouping in select widgets will show all events associated with that widget.

The following table lists the widgets you create, edit, and customize in the application.

Widget Type	Description
KPI	Displays metrics about the health and performance of the SEM appliance.
Proportional	Displays an overview of widget group sizes in assorted charts (donut chart, pie chart, horizontal bar chart, vertical bar chart).

Widget Type	Description
New Time Series - Long Term	Displays event data for up to the last seven days. This data includes a broad range of records with less granularity than short-term widgets.
New Time Series - Short Term	Displays more granularity by allowing you to select filter and property data for a specified number of groups. For example, you can display a timeline chart of failed log-ons for the designated groups.
New Nodes Table Widget	Displays a variety of properties for each node in your network, such as IP address, operating system, connector profile, status, and more.

 If you created custom widgets with the old Flash console, these are not automatically migrated to the current SEM Dashboard, and you will need to recreate them.

Available SEM widgets

The following table describes the customizable widgets that ship with the SEM Console.

Widget	Description
Active Directory Group Changes by Group	Displays a donut chart of group changes by group name.
Active Directory Group Changes by Type	Displays a donut chart of group changes by event type.
Active Directory Group Changes by User	Displays a pie chart of group changes by user source account.
Active Directory User Changes by Type	Displays a donut chart of user account changes by event type.
All Events - Last 12 Hours	Displays a time series view of all events occurring in the last 12 hours.
All Events - Last 24 Hours	Displays a time series view of all events occurring in the last 24 hours.
All Events by Connector Name	Displays a pie chart of all events by connector name using the ToolAlias log property.
All Events by Event Type	Displays a donut chart of the number of all event types.
Blocked Web Traffic by Source Machine	Displays a donut chart of the top sources of blocked web traffic.

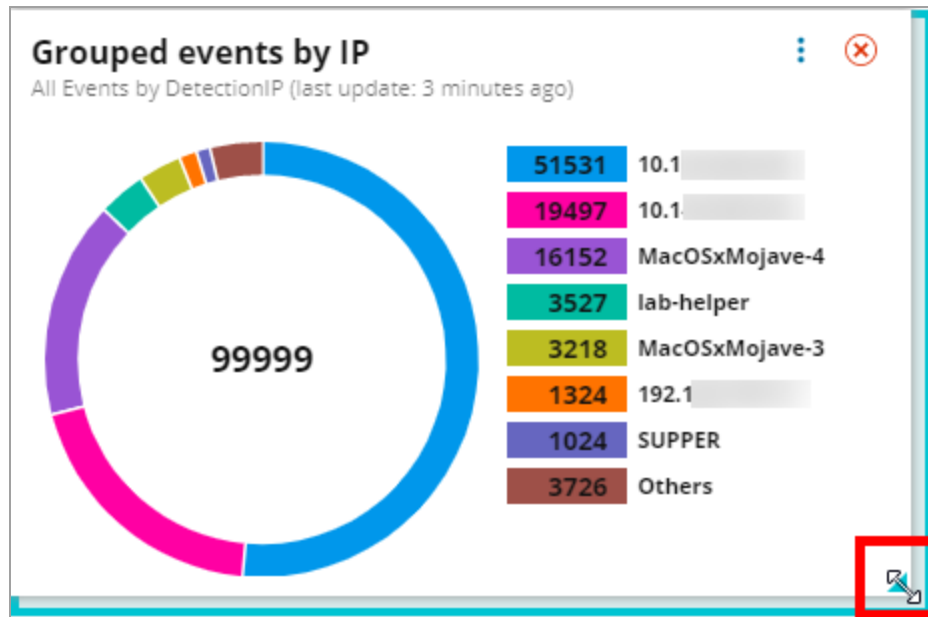
Widget	Description
Events Per Second - Last Hour	Displays the total count of events per second for the past hour.
File Audit Failures by User	Displays a donut chart of the file audit failure events by user.
Firewall Events by Type	Displays a donut chart of the top firewall events by event type.
Grouped events by IP	Displays a donut chart of group events by detection IP.
HIPAA Events by Type	Displays a pie chart of top HIPAA events by event type.
Incidents by Rule Name	Displays a pie chart of incidents by inference rule.
Interactive Logons by User	Displays a vertical bar chart of user logons by destination account.
KPI	Displays key performance indicators (KPIs) related to SEM appliance performance, including EPS and resource consumption.
Log Database Used Storage Percent	Displays the logs/data used percentage (KPI widget) with an 80 percent warning threshold and a 90 percent critical threshold.
Logon Failures - Last 24 Hours	Displays a time series chart of failed logons for the past 24 hours.
Logon Failures by Reason	Displays a pie chart of failed logons by failure reason.
Logon Failures by Source Machine	Displays a pie chart of failed logons by destination machine.
Logon Failures by User	Displays a horizontal bar chart of failed logons by destination account.
Node Health	Displays a table of the latest events from monitored network nodes.
PCI Events by Type	Displays a donut chart of the top PCI events by event type.
Proportional	Displays log data using pie, bar, and donut charts.
Rules Fired by Rule Name	Displays a pie chart of rule activity by inference rule.

Widget	Description
Scheduled query severity per tag	Displays a pie chart with the total number of severities (such as Critical, Warning, and OK) for each tag.
Scheduled query table severity per tag	Displays a table with a list of severities for each tag. The table includes the query name, severity, event count, and execution date.
Table	Displays a table with a list of selected nodes.
Time Series - Long Term	Adds key metrics related to long term SEM appliance performance, including EPS and resource consumption.
Time Series - Short Term	Adds key metrics related to short term SEM appliance performance, including EPS and resource consumption.
Threat Events by Type	Displays a pie chart of threat events by event type.
Traffic by Destination Port	Displays a vertical bar chart of all network traffic by destination port.
Traffic by Source Port	Displays a vertical bar chart of all network traffic by source port.
User Account Changes by Destination Account	Displays a horizontal bar chart of all user account changes by destination account.
User Account Changes by Source Account	Displays a horizontal bar chart of all user account changes by source account.
User Logon by Source Machine	Displays a donut chart of all user logons by source machine.
User Logon by User	Displays a donut chart of user logons by destination account.
Virus Attacks by Machine	Displays a pie chart of virus attacks by source machine.
Virus Attacks by Virus Name	Displays a pie chart of virus attacks by virus name.

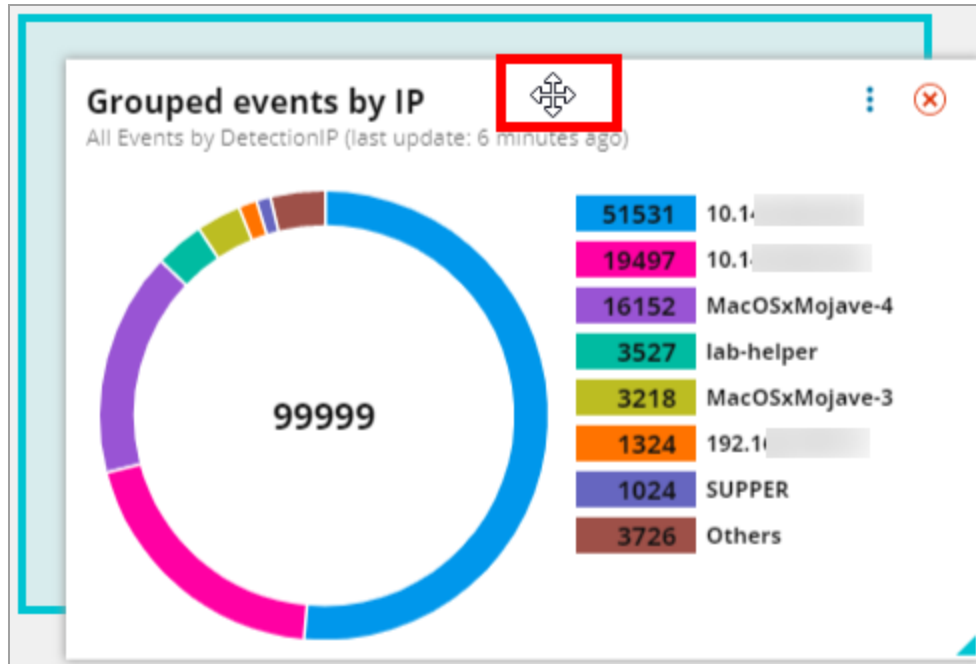
Edit the SEM dashboard

Place the SEM Dashboard in edit mode to reorganize and resize widgets, edit widget properties, and add or remove widgets.

1. On the SEM Console, click the Dashboard tab.
2. On the upper right of the SEM Dashboard, click Edit Dashboard.
3. To resize a widget, drag the lower-right corner to increase or decrease the size.



- To move a widget, drag the widget header to a different location on the SEM Dashboard.

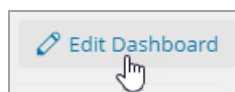


 In edit mode, you can also, [add](#), [edit](#), and [remove](#) widgets.

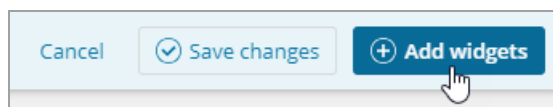
- After you complete your edits, click Done editing on the Edit dashboard toolbar.

Add dashboard widgets

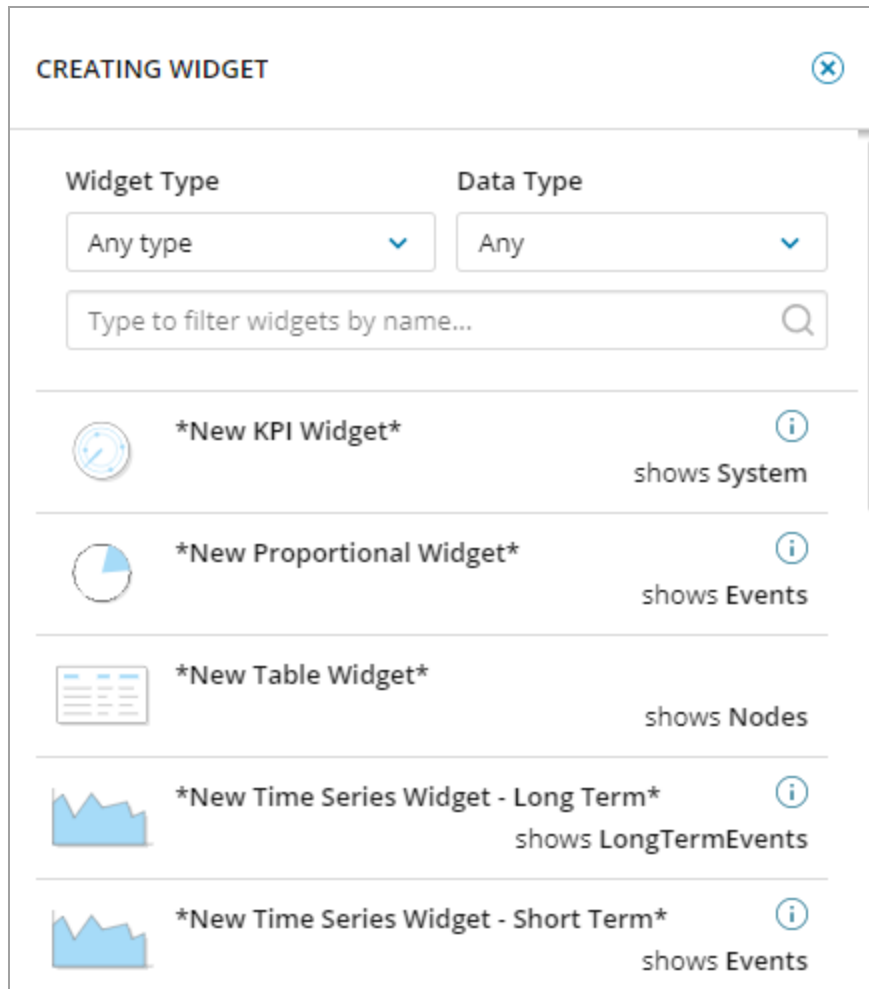
- [Log in to the SEM Console.](#)
- On the Dashboard toolbar, click Edit Dashboard.



- On the Edit Dashboard toolbar, click Add widgets.

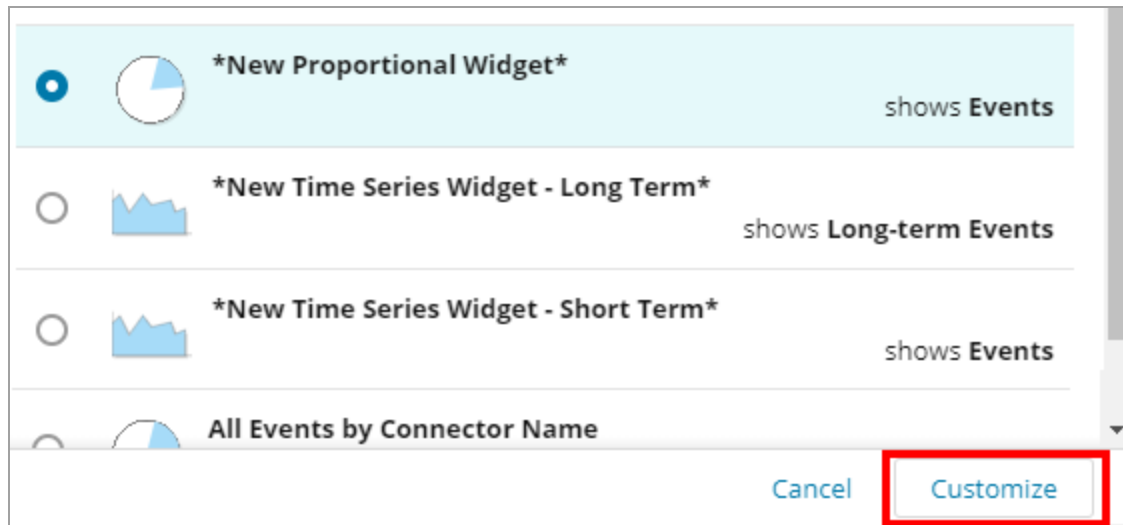


The Creating Widget pane expands displaying a variety of widgets and widget templates.



4. Click the Widget type drop-down menu and select a widget category.
5. Click the Data Type drop-down menu and select Any, Events, or Nodes.
6. In the Search field, enter a term to refine your search.

7. Select a widget template (for example, New Proportional Widget), and then click Customize.



8. Click the edit icon  in each template section to name the widget, add widget features, and establish the graphic style and content derived from the designated data source. You can click Filter and Properties to set the values based on your existing Event table filters.

For example, to view the number of logon failures and the failure reason, set your filter to `Failed Logons` and your properties to `FailureReason`.

CREATING WIDGET

Presentation

 **Title and Description**
Empty Proportional Widget, Failed Logons by Fail...

 **Filter and property**
Failed Logons by FailureReason

Filters

Failed Logons

Properties

FailureReason

Number of shown groups

10

 **Chart Options**
Donut

 **Refresh**
enabled, 30sec

Cancel

< Back

Create Widget



- The filter and properties are the primary values that populate widgets. You can create and customize numerous widgets to present key data points associated with your network environment. See the Filters pane in the Events tab to review specific event filters to use when customizing your widgets. See [About SEM features](#) for more information.
- The number of events that display in your widgets are established in your filter threshold settings.

9. Click the arrows to set the number of groups to display in your widget.

10. Select your chart type (Donut, Pie, Horizontal, or Vertical), legend, and refresh rate. As you make your changes, the widget preview updates to the left of the widget template.

 The data refresh rate is set to 30 seconds by default. You can increase the refresh rate up to one hour or decrease it to one second.

11. Click Create Widget, and then click Save changes.

The new widget displays on the SEM dashboard.

12. [Move and resize the widget](#) as needed.

To edit the widget (in edit mode), click the vertical ellipsis on the upper right of the widget and select Edit widget.

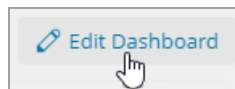


To leave edit mode, click Save changes on the Edit dashboard toolbar.

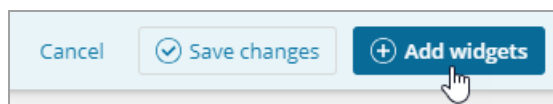
To view the associated widget records in the Events viewer, click the widget chart.

Edit the dashboard widgets

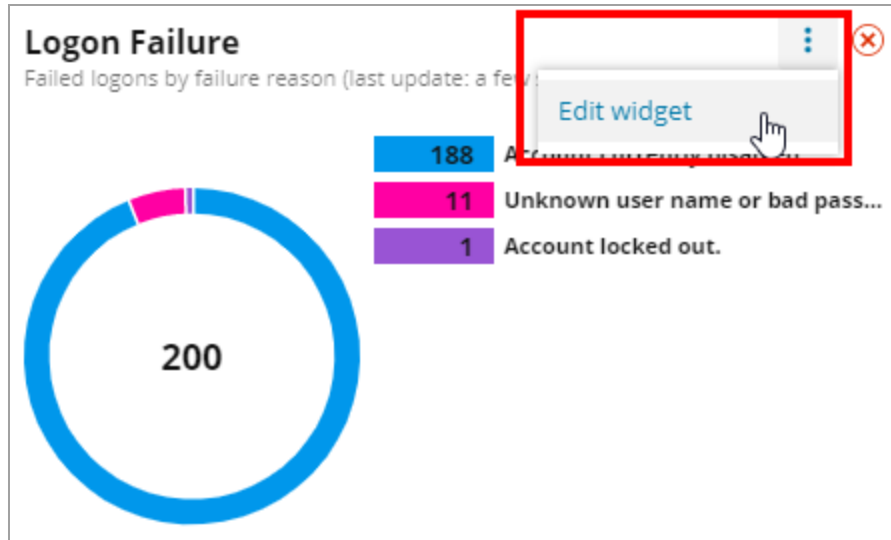
1. [Log in to the SEM Console.](#)
2. On the Dashboard toolbar, click Edit Dashboard.



3. On the Edit Dashboard toolbar, click Add widgets.



- Click the vertical ellipsis on the upper right of the widget and select Edit widget.



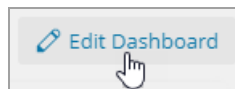
To remove a widget, click the Remove Widget button .

Create a KPI widget

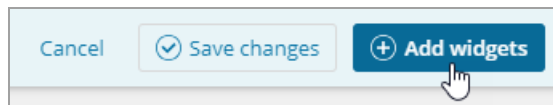
The KPI widget displays up-to-date metrics on the health and performance of your SEM appliance.

 Starting with version 2020.2, SEM introduces a new data indicator to the KPI widget that displays the age of the oldest stored event in your database. This can be especially helpful when managing database storage and adjusting your data retention settings.

- [Log in to the SEM Console.](#)
- On the Dashboard toolbar, click Edit Dashboard.



- On the Edit Dashboard toolbar, click Add widgets.



The Creating Widget pane expands, displaying a variety of widgets and widget templates.

CREATING WIDGET

Widget Type
Data Type

Any type
Any

Type to filter widgets by name...



New KPI Widget

shows System



New Proportional Widget

shows Events



New Table Widget

shows Nodes



New Time Series Widget - Long Term

shows LongTermEvents



New Time Series Widget - Short Term

shows Events

4. Select ***New KPI Widget***, and then click **Customize**.
5. Expand **Title and Description**, and enter a title for the widget (subtitle and description are optional).
6. Click **Add New Value** to set your **Description**, **Indicator Data**, and **Threshold** values for a specific data set. For example:
 - a. Expand **Data Source**, and select **Logs/Data used storage percentage** from the dropdown. This option allows you to monitor the amount of free storage space.
 - b. Expand **Thresholds**, and select **Use custom thresholds** to establish notifications when storage space is low. For example, you can set the warning to 80 percent full, and critical to 90 percent full.
7. Continue to add more values to monitor in the KPI widget, such as events per second or manager memory used. As you continue to add values, The widget preview updates to the left of the widget template.

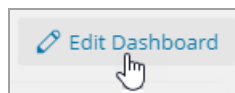


8. To add your KPI widget to the dashboard, click Create Widget, and then click Save changes.

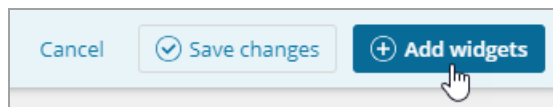
Create a time-series widget

You can create interactive time-series widgets view data points at specific time intervals. Use long-term widgets for view a broader range of records (up to seven days). Use short-term widgets to drill down into specific log activity over a designated time.

1. [Log in to the SEM Console.](#)
2. On the Dashboard toolbar, click Edit Dashboard.



3. On the Edit Dashboard toolbar, click Add widgets.



The Creating Widget pane expands displaying a variety of widgets and widget templates.

4. Select New Time Series Widget - Short Term*, and then click Customize.

CREATING WIDGET

Presentation

Title and Description

Empty Timeseries Widget,

Filter and property

Timeseries metadata

Last 7 days, None, No y-axis label

Refresh

enabled, 30sec

Cancel

< Back

Create Widget

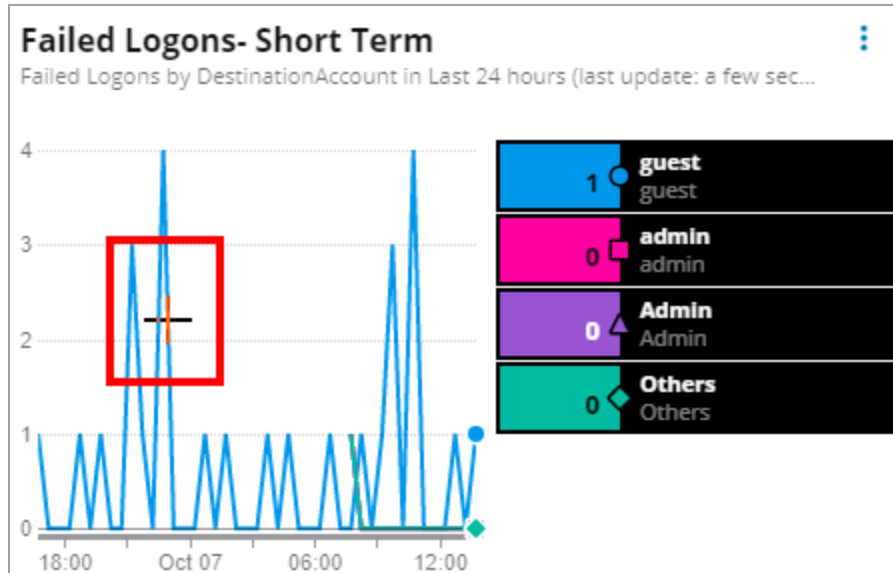
 To monitor a broader range of event logs, select the long-term widget.

5. Expand Title and Description, and enter a title for the widget (subtitle and description are optional).
6. Expand the Filter and property section.
 - a. From the drop-down lists, select the specific event groupings to appear in the widget. For example, if you want to monitor a time line of failed logons, select Failed Logons from the Filters drop-down list, and then select DestinationAccount from the properties drop-down list.
 - b. Click the arrows to set your number of shown groups (between one and 10).
7. Expand the Timeseries Metadata section, and select your starting time span, chart legend display option, and then the auto refresh rate.

 As you make your changes, the widget preview updates to the left of the widget template.

8. Click Create Widget, and then click Save changes.

- To view event logs for a designated time, click a specific point in the chart.



The Events viewer opens displaying associated logs.

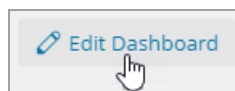


NAME	EVENT INFO	DETECTION IP	DETECTION TIME
UserLoginFailure	Login Failure "guest"	SE-EMEA-0026.emea.sales	2019-10-06 22:54:42
UserLoginFailure	Login Failure "guest"	SE-EMEA-0026.emea.sales	2019-10-06 22:44:41
UserLoginFailure	Login Failure "guest"	SE-EMEA-0026.emea.sales	2019-10-06 22:43:27
UserLoginFailure	Login Failure "guest"	SE-EMEA-0026.emea.sales	2019-10-06 22:41:51

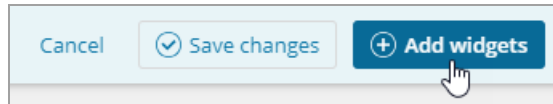
Create a nodes table widget

The nodes table widget displays a variety of properties for each node in your network, such as IP address, operating system, connector profile, status, and more.

- [Log in to the SEM Console.](#)
- On the Dashboard toolbar, click Edit Dashboard.

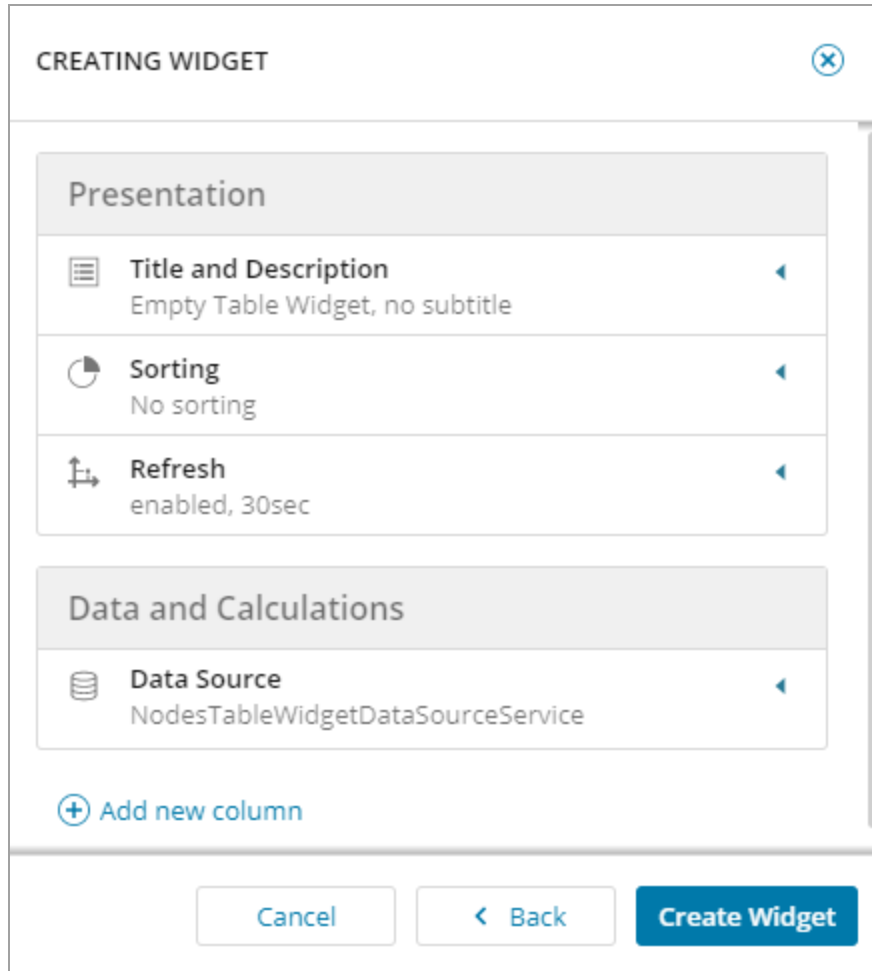


3. On the Edit Dashboard toolbar, click Add widgets.



The Creating Widget pane expands displaying a variety of widgets and widget templates.

4. Select New Table Widget and then click Customize.



5. Expand Title and Description and enter a title for the widget (subtitle and description are optional).
6. Expand Sorting, and select a sorting option.
7. Under Refresh, enable Refresh if required and set the refresh rate.
8. To add values and formatting to each column, select Add New Column.
9. Expand Description, and enter the column name.
10. Expand Property, and select the format and column value from the drop-downs .

11. Continue to add columns and values. As you make your changes, the widget preview updates to the left of the widget template.
12. To add your widget to the dashboard, click Create Widget, and then click Save changes.

Manage SEM users

This section describes how to add SEM users, view system privileges, and manage user access to the application.

Add SEM users

Access to SEM data requires a user account. Even basic access, such as receiving notifications sent by SEM through email or SMS text message, requires a user account.

About SEM roles

To restrict user access to sensitive data, user accounts need to be assigned to a SEM role. There are six SEM role types: Administrator, Auditor, Monitor, Guest, Reports, and Contact. Role types are described in the following table.

See [View system privileges associated to roles](#) for more information.

Role	Description
Administrator	The default user. This role cannot be deleted and has full access to the SEM console.  SolarWinds does not recommend multiple users sharing the Admin account for auditing purposes.
Auditor	User has extensive view rights to the system, but cannot modify anything other than their own filters.
Monitor	User has read-only access to the SEM console. See Monitor role users and filters to configure the filters assigned to this role. Users assigned to this role cannot edit filters.
Guest	User has extensive view rights to the system, but cannot modify anything other than their own filters.
Contact	User cannot log in to the SEM console, but can receive external notifications such as email sent to either the user's email address, imported distribution lists, or cellular email-to-SMS addressees for texts. Use this role if you have an external incident resolution or trouble ticket system, or if you have a user who does not need to access the console.
Reports	User can access the SEM Console and generate query reports.

- i** Do not confuse roles and groups:
- Roles restrict the actions a user can perform in SEM.
 - Groups organize related elements into logical units so that they can be used in SEM rules and filters.

About SEM user accounts

There are two ways to add a user account in SEM:

- Add an Active Directory user account
- Create a local user account

- i** SolarWinds recommends using Active Directory accounts if Microsoft Active Directory is in use at your organization.

Each user should have a valid email address so that the user can receive notifications sent by SEM. SolarWinds recommends that you create distinct users for everyone who needs to receive email notifications from SEM Manager. If you want to send identical notifications to your IT department personnel, associate a distribution list email address to all relevant users.

- i** See [Set the global password policy for SEM users](#) for details about establishing minimum requirements for local SEM user accounts.

How Active Directory accounts work in SEM

You can configure SEM to allow users to log in with their Active Directory credentials. Using Active Directory for user authentication means you do not have to maintain duplicate user accounts in SEM, and users do not have to remember an additional user name and password just for SEM.

- i** See [Set up Active Directory authentication in SEM](#) to configure SEM to allow users to log in with their Active Directory credentials.

SEM roles are mapped to DS groups in Active Directory if AD authentication is enabled.

- i** See [Set up Active Directory authentication in SEM](#) to look up which Active Directory groups are mapped to SEM roles.

SEM supports Active Directory single sign-on (SSO). If SSO is enabled, users can bypass the SEM login screen and go straight to the application if they are already logged in to another application that accepts the user's AD credentials.

 See [Set up single sign-on in SEM](#) to configure SEM to allow users to bypass the SEM login screen if they are already logged in to an application that accepts the user's AD credentials.

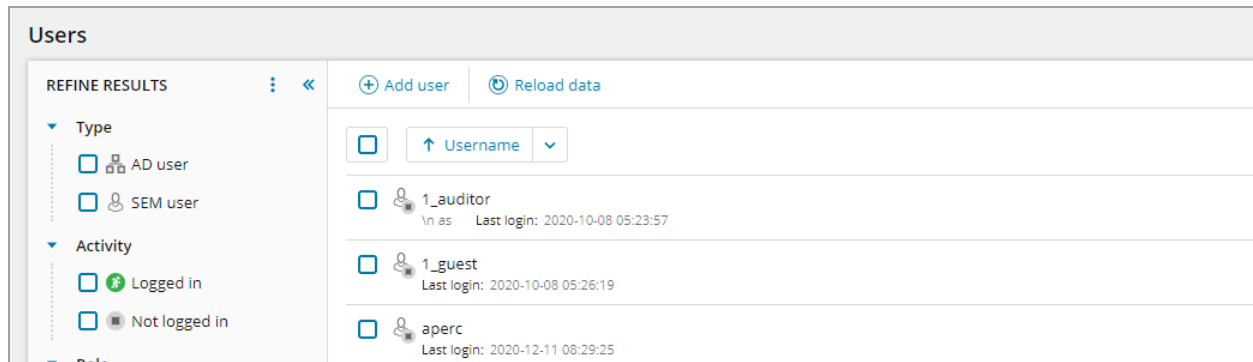
SEM can use Active Directory groups of Windows users and computer accounts in SEM rules and filters. Any changes made to users or groups in Active Directory propagate to rules and filters in SEM.

Create a local SEM user account

Access to SEM data requires a user account. Even basic access, such as receiving notifications sent by SEM through email or SMS text message, requires a user account.

User accounts need to be assigned to a SEM role to restrict access to sensitive data. There are five SEM role types: Administrator, Auditor, Monitor, Guest, and Reports. Role types are described in the following table.

1. On the SEM Console, navigate to Configure > Users.



2. On the Users toolbar, click Add user.
3. Complete the user account form, and then click Add. Reference the table below for information on the form fields.

Field	Description
Username	User account name.

Field	Description
Password	User password to access the Manager. This can be an initial system password or a temporary password that is assigned to replace a forgotten password. If password restrictions are enabled ( > Authentication > Local Users), SEM enforces the following policy: Passwords must: • Be between 6-40 characters • Not include user names • Not include forbidden characters Passwords must also include at least three of the following: • One upper case letter • One lower case letter • One special character • One digit
Confirm password	Enter the password again.
Role	Select a SEM role for this user. • Administrator - Has full access to the system, and can view and modify everything. • Auditor - Has extensive view rights to the system, but cannot modify anything other than their own filters. • Monitor - Can access the console, cannot view or modify anything, and must be provided a set of filters. See "Specify the filters that users assigned the Monitor role can use on the SEM Console" for steps. • Guest - Has extensive view rights to the system, but cannot modify anything other than their own filters. • Reports - Can log in to the SEM console and generate reports. This role can access the SEM database over a secure channel.
First name	User's first name
Last name	User's last name
Description	Type a brief description (up to 50 characters). For example, provide the user title, position, or area of responsibility.

Field	Description
Contact e-mail	Email address. SEM notifies users by email about network security events. You can add as many email addresses as required.

4. Select a user in the list to edit the user account, change the user's password, require the user to change passwords, or delete the user account.



In the Refine Results pane, you can filter users based on account type and last login. Under Last modified, click the time setting to adjust the login time frame.

Edit user account settings

1. On the SEM Console, click the Configure tab, and select Users from the drop-down list.
2. Select a user account in the list:
 - To edit the user account settings, click Edit user.
 - To remove a local user account from the system, click Delete.
 - To change a user's password, click Change password, then enter and confirm the password in the pop-up window.
 - To require that a user change their password when first logging in, click Require password change.

View system privileges associated with a role

Below are the system privileges associated with a user role. Privileges are either allowed , not allowed , or not applicable . The following roles are available:

- [Admin](#)
- [Auditor](#)
- [Monitor](#)
- [Guest](#)
- [Reports](#)
- [Contact](#)

Admin

Area	Access	Modify	Audit
General			

Area	Access	Modify	Audit
Options	✓	✓	✓
Add Agents	✓	✓	✓
Remove agents	✓	✓	✓
Users	✓	✓	✓
Policy	✓	✓	✓
Database warehouse	✓	✓	✓
Actions	✓	✓	✓
Explorer			
Nslookup	✓	✓	✓
Traceroute	✓	✓	✓
Whois	✓	✓	✓
Get IP information	✓	✓	✓
Tools			
Manager tools	✓	✓	✓
Agent tools	✓	✓	✓
Tool profile tools	✓	✓	✓
Groups			
Alert groups	✓	✓	✓
Directory service groups	✓	✓	✓
Time-of-day sets	✓	✓	✓
Tool profiles	✓	✓	✓
User-defined groups	✓	✓	✓
Properties			
Manager status	✓	⚠	✓
Manager tools	✓	⚠	✓

Area	Access	Modify	Audit
Manager remote updates	✓	✓	✓
Agent status	✓	✗	✓
Agent tools	✓	✗	✓
Agent remote updates	✓	✓	✓
Filters			
Filter Editor	✓	✓	✓
Organize	✓	✓	✓
Rename	✗	✓	✓
Export	✗	✓	✓
Import	✗	✓	✓
Clone	✗	✓	✓
Delete	✗	✓	✓
Enable/disable	✗	✓	✓
Rules			
Rule Editor	✓	✓	✓
State variables	✓	✓	✓
Notification templates	✓	✓	✓
FIM			
FIM driver controls	✓	✓	✓
Reports			
Report viewer	✓	✓	✓

[Return to top](#)

Auditor

Area	Access	Modify	Audit
General			
Options	✓	✗	✓
Add Agents	✓	✗	✓
Remove agents	⚠	✗	✓
Users	✓	✗	✓
Policy	✓	✗	✓
Database warehouse	✓	✗	✓
Actions	⚠	✗	✓
Explorer			
Nslookup	⚠	✓	✓
Traceroute	⚠	✓	✓
Whois	⚠	✓	✓
Get IP information	⚠	✓	✓
Tools			
Manager tools	✓	✗	✓
Agent tools	✓	✗	✓
Tool profile tools	✓	✗	✓
Groups			
Alert groups	✓	✗	✓
Directory service groups	✓	✗	✓
Time-of-day sets	✓	✗	✓
Tool profiles	✓	✗	✓
User-defined groups	✓	✗	✓
Properties			

Area	Access	Modify	Audit
Manager status	✓	⚠	✓
Manager tools	✓	⚠	✓
Manager remote updates	✓	✗	✓
Agent status	✓	⚠	✓
Agent tools	✓	⚠	✓
Agent remote updates	✓	✗	✓
Filters			
Filter Editor	✓	✓	✓
Organize	✓	⚠	✓
Rename	⚠	✓	✓
Export	⚠	✓	✓
Import	⚠	✓	✓
Clone	⚠	✓	✓
Delete	⚠	✓	✓
Enable/disable	⚠	✓	✓
Rules			
Rule Editor	✓	✗	✓
State variables	✓	✗	✓
Notification templates	✓	✗	✓
FIM			
FIM driver controls	✗	✗	✗
Reports			
Report viewer	✓	✓	✓

[Return to top](#)

Monitor

Area	Access	Modify	Audit
General			
Options	✗	✗	✓
Add Agents	✗	✗	✓
Remove agents	⚠	✗	✓
Users	✗	✗	✓
Policy	✗	✗	✓
Database warehouse	✗	✗	✓
Actions	⚠	✗	✓
Explorer			
Nslookup	⚠	✗	✓
Traceroute	⚠	✗	✓
Whois	⚠	✗	✓
Get IP information	⚠	✗	✓
Tools			
Manager tools	✗	✗	✓
Agent tools	✗	✗	✓
Tool profile tools	✗	✗	✓
Groups			
Alert groups	✗	✗	✓
Directory service groups	✗	✗	✓
Time-of-day sets	✗	✗	✓
Tool profiles	✗	✗	✓
User-defined groups	✗	✗	✓
Properties			

Area	Access	Modify	Audit
Manager status			
Manager tools			
Manager remote updates			
Agent status			
Agent tools			
Agent remote updates			
Filters			
Filter Editor			
Organize			
Rename			
Export			
Import			
Clone			
Delete			
Enable/disable			
Rules			
Rule Editor			
State variables			
Notification templates			
FIM			
FIM driver controls			
Reports			
Report viewer			

[Return to top](#)

Guest

Area	Access	Modify	Audit
General			
Options	✓	✗	✓
Add Agents	✓	✗	✓
Remove agents	⚠	✗	✓
Users	✓	✗	✓
Policy	✓	✗	✓
Database warehouse	✓	✗	✓
Actions	⚠	✗	✓
Explorer			
Nslookup	⚠	✓	✓
Traceroute	⚠	✓	✓
Whois	⚠	✓	✓
Get IP information	⚠	✓	✓
Tools			
Manager tools	✓	✗	✓
Agent tools	✓	✗	✓
Tool profile tools	✓	✗	✓
Groups			
Alert groups	✓	✗	✓
Directory service groups	✓	✗	✓
Time-of-day sets	✓	✗	✓
Tool profiles	✓	✗	✓
User-defined groups	✓	✗	✓
Properties			

Area	Access	Modify	Audit
Manager status	✓	⚠	✓
Manager tools	✓	⚠	✓
Manager remote updates	✓	✗	✓
Agent status	✓	⚠	✓
Agent tools	✓	⚠	✓
Agent remote updates	✓	✗	✓
Filters			
Filter Editor	✓	✓	✓
Organize	✓	⚠	✓
Rename	⚠	✓	✓
Export	⚠	✓	✓
Import	⚠	✓	✓
Clone	⚠	✓	✓
Delete	⚠	✓	✓
Enable/disable	⚠	✓	✓
Rules			
Rule Editor	✓	✗	✓
State variables	✓	✗	✓
Notification templates	✓	✗	✓
FIM			
FIM driver controls	✗	✗	✗
Reports			
Report viewer	✗	✗	✗

[Return to top](#)

Reports

Area	Access	Modify	Audit
General			
Options			
Add Agents			
Remove agents			
Users			
Policy			
Database warehouse			
Actions			
Explorer			
Nslookup			
Traceroute			
Whois			
Get IP information			
Tools			
Manager tools			
Agent tools			
Tool profile tools			
Groups			
Alert groups			
Directory service groups			
Time-of-day sets			
Tool profiles			
User-defined groups			
Properties			

Area	Access	Modify	Audit
Manager status			
Manager tools			
Manager remote updates			
Agent status			
Agent tools			
Agent remote updates			
Filters			
Filter Editor			
Organize			
Rename			
Export			
Import			
Clone			
Delete			
Enable/disable			
Rules			
Rule Editor			
State variables			
Notification templates			
FIM			
FIM driver controls			
Reports			
Report viewer			

[Return to top](#)

Contact

Area	Access	Modify	Audit
General			
Options			
Add Agents			
Remove agents			
Users			
Policy			
Database warehouse			
Actions			
Explorer			
Nslookup			
Traceroute			
Whois			
Get IP information			
Tools			
Manager tools			
Agent tools			
Tool profile tools			
Groups			
Alert groups			
Directory service groups			
Time-of-day sets			
Tool profiles			
User-defined groups			
Properties			

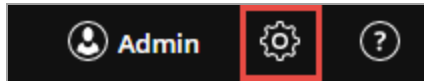
Area	Access	Modify	Audit
Manager status			
Manager tools			
Manager remote updates			
Agent status			
Agent tools			
Agent remote updates			
Filters			
Filter Editor			
Organize			
Rename			
Export			
Import			
Clone			
Delete			
Enable/disable			
Rules			
Rule Editor			
State variables			
Notification templates			
FIM			
FIM driver controls			
Reports			
Report viewer			

[Return to top](#)

Set the global password policy for SEM users

In the Authentication settings, you can set minimum password requirements for local SEM user accounts.

1. On the SEM Console, click the Settings button.



2. On the Settings page, click the Authentication tab, and then select Local Users.
3. To require complex passwords for SEM users, click the Password Restrictions toggle button.

i Passwords should be at least nine-characters long, cannot contain user names or control characters, or be longer than 40 characters.

Complex passwords must include any three of the following four character types:

- One upper-case letter
- One lower-case letter
- One Number
- One special character (!, @, #, etc.)

4. Adjust the Minimum Password Length setting according to your preference, and then click Save.

Set up Active Directory authentication in SEM

Set up Active Directory authentication to allow users to log in to SEM with their Active Directory (AD) credentials.

i This task configures SEM for Active Directory authentication. See [Configure Active Directory and SEM to work with SEM rules and filters to configure SEM to monitor Active Directory accounts for security violations](#).

Gather required information

Before you begin, gather the following:

- Either the IP address or fully-qualified domain name (FQDN) of the Active Directory server.
- The domain credentials for an account that SEM can use to log in to Active Directory. SolarWinds recommends using a service account with a non-expiring password. This account does not need elevated privileges.

 To get directory server details, open a Windows command prompt on a computer on the correct network and type `nslookup`.

Create a user in Active Directory that SEM can use to log in

1. Log in to the domain controller and open Active Directory Users and Computers.
2. Create a user account that SEM can use to log in to Active Directory. SolarWinds recommends using a service account with a non-expiring password. This account does not need elevated privileges (such as Domain Admin privileges).

Create custom security groups in Active Directory for SEM to use

User access in SEM is based on Active Directory group membership.

 If you are using your existing Active Directory groups for alerts, reports, and so on, skip this section and go to [Configure or view Active Directory authentication settings in SEM](#).

1. Log in to the domain controller and open Active Directory Users and Computers.
2. Create at least one security group called `ROLE_LEM_ADMINISTRATORS`. Group names must be identical to the names given below, otherwise users cannot log in to the SEM console. SolarWinds recommends creating SEM group names using capital letters to help you quickly identify SEM groups in Active Directory.

You can add up to six of the following SEM custom groups:

- `ROLE_LEM_ADMINISTRATORS`
- `ROLE_LEM_ALERTS_ONLY`

 `LEM_ALERTS_ONLY` permissions correspond with the monitor user role.

- `ROLE_LEM_AUDITOR`
- `ROLE_LEM_GUESTS`
- `ROLE_LEM_CONTACTS`
- `ROLE_LEM_REPORTS`

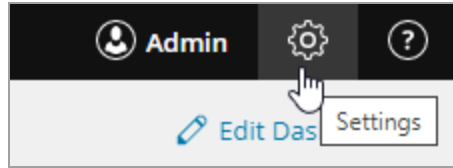
Learn more about SEM roles [here](#).

 The `ROLE_LEM_CONTACTS` group is only used for email notification in rules. Users added to this group do not have login rights.

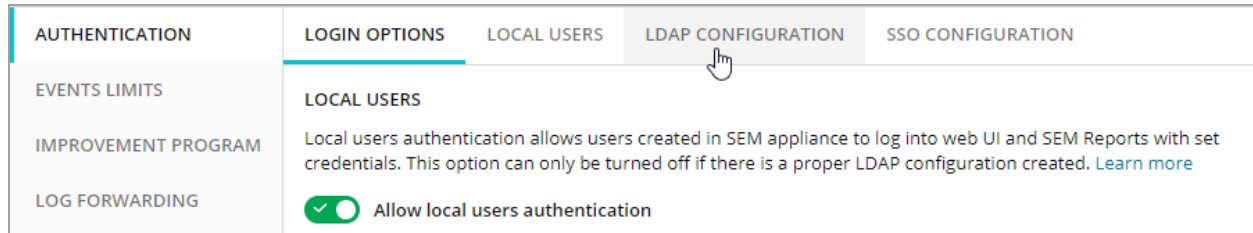
Configure or view Active Directory authentication settings in SEM

In SEM 2020.4 and newer versions, you can create multiple LDAP configurations.

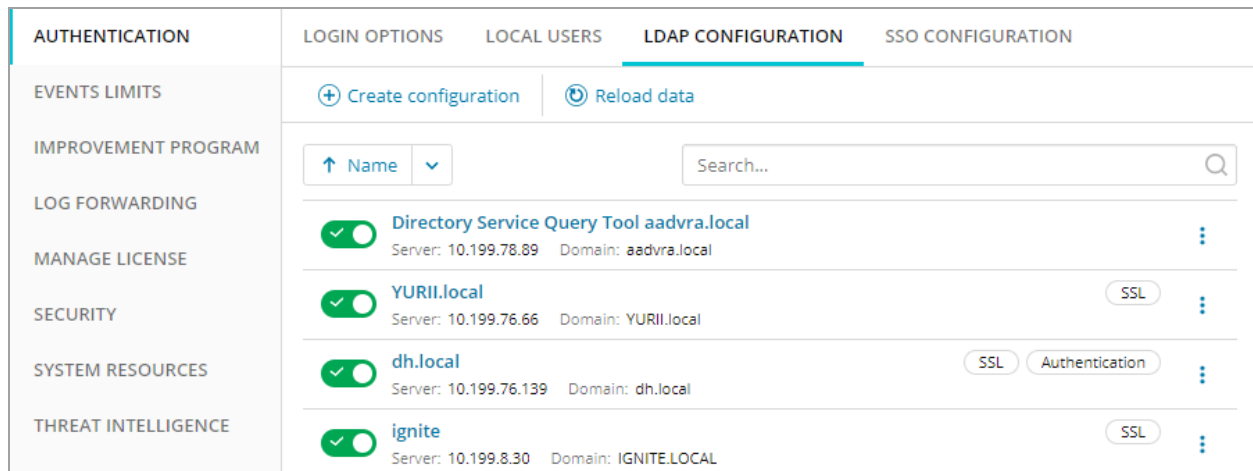
1. Click the settings icon on the upper right.



2. Select Authentication > LDAP Configuration.



If any LDAP configurations have already been created these are displayed.



3. Click Create configuration.

The Create LDAP Configuration dialog is displayed.

Create LDAP Configuration

Configure LDAP

Confirm Certificate

Summary

Configure LDAP

Configuration Name

This is required

IP or Hostname

Domain

Directory Service Server User Name

Directory Service Server Password

Use SSL Encryption

LDAP Port

Cancel

Next >

4. Enter the required information.

See the table below.

Field	Description
Configuration Name	Enter a friendly name of your choosing for the LDAP configuration.
IP or Hostname	Enter the IP address or host name of your LDAP server.
Domain	Enter the fully-qualified domain name for the account store.
Directory Service Server User Name	Use the format account_name@example.com. SolarWinds recommends using a Directory Service account to prevent integration issues if the software license expires. The user name does not require special privileges (such as Domain Admin) to be a Directory Service user.
Directory Service Server Password	Enter the password for the user account.
Use SSL Encryption	(Optional) Select to use the transport layer security protocol (LDAPS) for a secure connection. This option directs traffic from the SEM VM to a designated server (usually a domain controller) for use with the Directory Service tool.
LDAP Port	If SSL encryption is not used, the default for this setting is 389. If SSL encryption is used, the default for the port is 636.
Use for Authentication	Select, then click Next if you wish to use Advanced Settings shown below.
Domain Aliases (Optional)	Specify any Domain Alias names that should be authenticated using this LDAP configuration. (The role/group names configured on this page will also apply.)
NetBIOS Names (Optional)	Specify any NetBIOS names that should be authenticated using this LDAP configuration. (The role/group names configured on this page will also apply.)
Admin Group (Optional)	Specify the DS group in Active Directory to use for the SEM administrator role. If you do not specify a name, the default ROLE_LEM_ADMINISTRATORS group is used.

Field	Description
Alerts Only Group (Optional)	Specify the DS group in Active Directory to use for the SEM auditor role. If you do not specify a name, the default ROLE_LEM_AUDITOR group is used.
Guest Group (Optional)	Specify the DS group in Active Directory to use for the SEM guest role. If you do not specify a name, the default ROLE_LEM_GUESTS group is used.
Notify Only Group (Optional)	Specify the DS group in Active Directory to use for the SEM notifications role. If you do not specify a name, the default ROLE_LEM_CONTACTS group is used.
Reports Group (Optional)	Specify the DS group in Active Directory to use for the SEM reports role. If you do not specify a name, the default ROLE_LEM_REPORTS group is used.

- Click Next.
- If you are using SSL encryption, the SSL certificate will be shown. Click I trust this certificate to confirm.
- Click Finish to create this configuration.
- Configurations can be sorted by name. For each configuration, the name, server, and domain are displayed, plus flags to show if they use SSL and/or used for Authentication.

Enable and disable LDAP configurations

Configurations are enabled as soon as they are created.

Use the toggles to disable or enable individual LDAP configurations.

 A warning message displays if you disable a configuration informing you that users will be unable to log on from that domain and any logged-in users from that domain will be immediately logged out.

Edit or delete an LDAP configuration

- To edit or delete an LDAP configuration, click on the vertical ellipsis icon after the configuration.



- Click Edit to display the Configure LDAP details for this configuration (which can now be edited

and saved).

Click Delete to remove this configuration.

Add an Active Directory user to SEM

To grant a user access to SEM, add the user to the appropriate role (security group) in Active Directory.

i SEM does not support nested Active Directory groups.

1. Open Active Directory Users and Computers.
2. Add the user to the appropriate role (security group) in Active Directory. Users added to the `ROLE_LEM_CONTACTS` group **do not** have sufficient privileges to log in to SEM.
3. Add the user to an Active Directory security group that is configured for use with SEM. To see which groups are configured for SEM, open the LDAP Configuration Management page and expand the list under Advanced Settings. See [Configure or View Active Directory settings in SEM](#) for details.

i When configuring user accounts, make sure the user's Primary group is not assigned to a custom group, otherwise the user cannot log in to SEM. The user will see an Invalid username and password message instead, and a message like the following will be logged:

```
[SemSpringSecurityAuthManager] {http-nio-8080-exec-1:349} Authentication
failed: User is not member of any required role group!
```

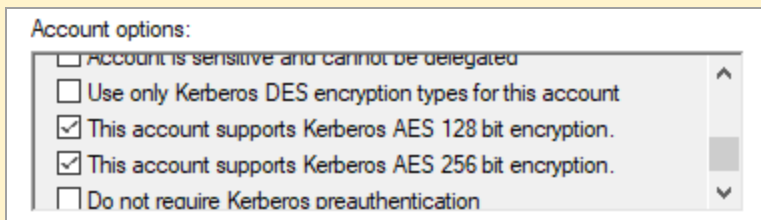
Set up single sign-on in SEM

SEM supports Active Directory (AD) single sign-on (SSO). When enabled, SEM does not request a user name and password if the user is already logged in to AD. Instead, AD authenticates the user in the background, and automatically logs the user in to SEM with the appropriate user access rights. User access on the SEM Console is based on AD group membership.

 With SEM 2022.2 and later, the weak, deprecated 3DES and RC4 Kerberos encryption types have been disabled by default. These have been replaced with AES-based encryption.

After upgrading to SEM 2022.2, users who were using 3DES or RC4 encryption will be unable to log into SEM using the SSO login. In this case, Kerberos AES encryption needs to be enabled in the respective Active Directory:

1. Locate the user account in Active Directory Users and Computers.
2. Select Properties.
3. Select the Account tab.
4. In the section titled Account Options, ensure one or both of the following options are selected.



To set up single sign-on:

1. [Enable Kerberos AES-based encryption](#)
2. [Set up Active Directory authentication in SEM](#)
3. [Generate a keytab file using Ktpass](#)
4. [Configure SSO settings](#)
5. [Configure browser settings for SSO](#)
6. [Configure SEM for either SSO-only authentication, or SSO and local authentication](#)
7. [Configure SSO settings in SEM using the command-line \(Deprecated\)](#)

Enable Kerberos AES-based encryption

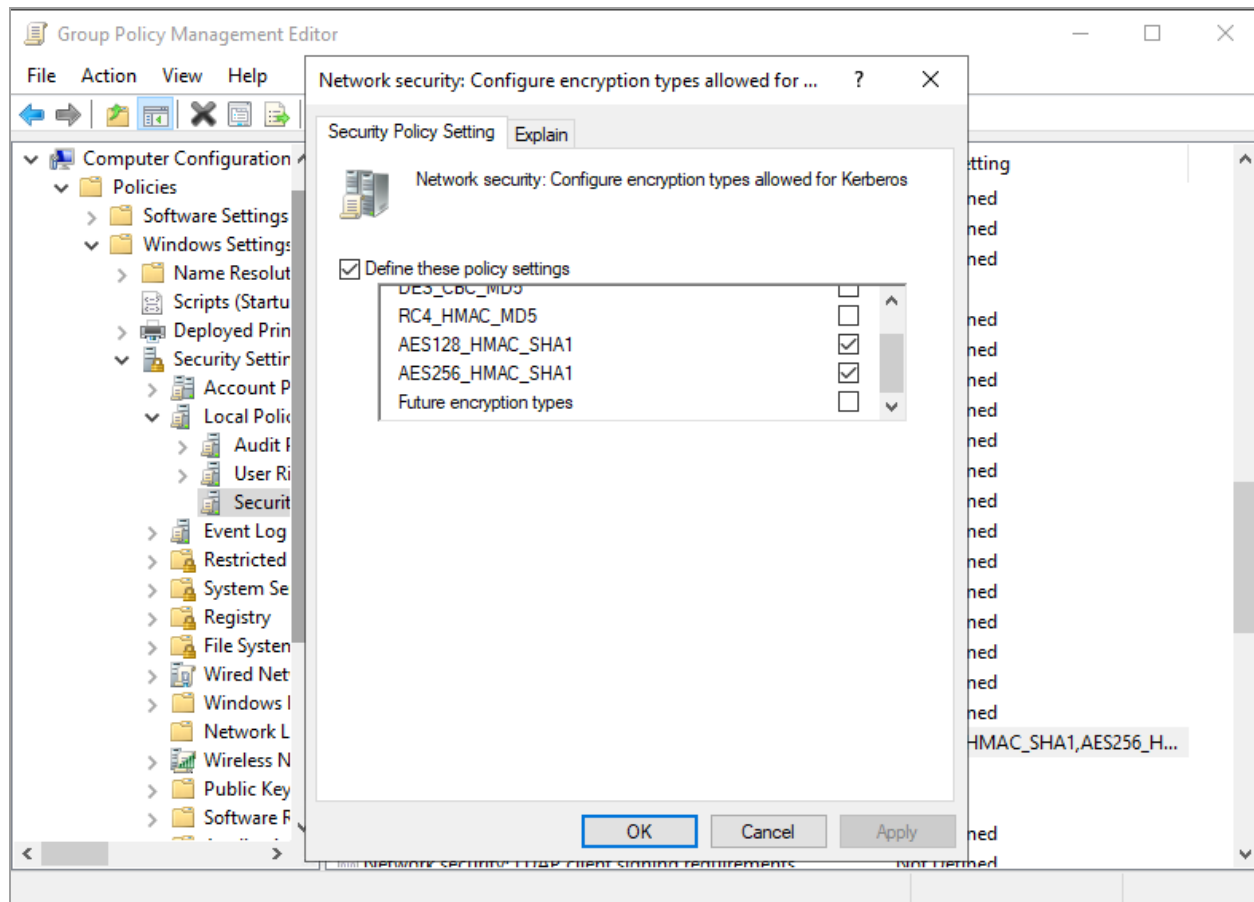
 In SEM 2022.2, the weak, deprecated 3DES and RC4 Kerberos encryption types have been disabled by default. These have been replaced with AES-based encryption.

After upgrading to SEM 2022.2, users who were using 3DES or RC4 encryption will be unable to log into SEM using the SSO login.

There are two options to enable Kerberos AES encryption:

For the whole Active Directory:

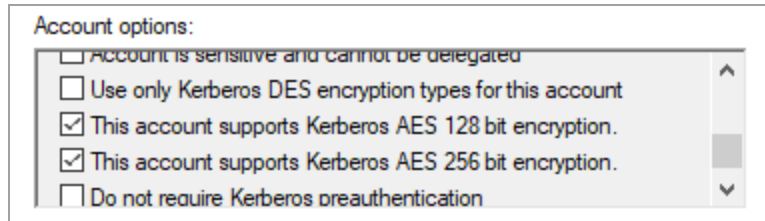
1. Open the Group Policy Management Console, locate the relevant domain and select Default Domain Policy
2. Right-click Default Domain Policy and select Edit.
3. Go to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options
4. Open Network security: Configure encryption types allowed for Kerberos:
 - Enable Define these policy settings.
 - Enable AES128_HMAC_SHA1.
 - Enable AES256_HMAC_SHA1.



For a single user in the Active Directory:

1. Locate the user account in Active Directory Users and Computers.
2. Select Properties.
3. Select the Account tab.

4. In the section titled Account Options, ensure the following options are selected.



Account options:

- ☐ Account is sensitive and cannot be delegated
- ☐ Use only Kerberos DES encryption types for this account
- ☒ This account supports Kerberos AES 128 bit encryption.
- ☒ This account supports Kerberos AES 256 bit encryption.
- ☐ Do not require Kerberos preauthentication

Set up Active Directory authentication in SEM

[Set up Active Directory authentication in SEM](#) and verify that users can log in to SEM with their AD credentials. When you are finished, [generate a keytab file using Ktpass](#).

Generate a keytab file using Ktpass

A Kerberos keytab file is required to configure SEM for AD SSO. SEM uses this file to authenticate users with AD and to enforce user account security. The keytab file is exported from AD and imported into SEM. The file contains a table of AD user accounts, along with the encrypted hash of each user's password. `ktpass` is the Windows Server command-line tool that generates the keytab file, as well as the shared secret key that SEM uses to securely authenticate users with AD.

 See [ktpass](#) located on the Microsoft Documentation website for information about the ktpass command and arguments.

Before you run the `ktpass` command, gather the following information:

- Fully-qualified domain name (FQDN) of the SEM VM – The FQDN is the complete domain name of the SEM virtual machine on the Internet. It includes the host name (the label assigned to a device on the network), and the name of the domain that hosts the device. For example, if the device name is `swi-sem` and the company domain is `yourcompany.local`, the FQDN is `swi-sem.yourcompany.local`.
- Realm – This is the Active Directory Domain Services (AD DS) domain name. The realm name is used to route authentication requests to the AD server that holds user credentials. The realm name is case sensitive and normally appears in upper-case letters. To simplify your Kerberos client configuration, make the realm name identical to your DNS domain name by only using upper-case letters. For example, if `YourCompany` belongs to the DNS domain name `yourcompany.com`, the Kerberos realm should be `YOURCOMPANY.COM`.
- Service principal name (SPN) – The SPN provides an alias (or *pointer*) to your domain account. The SPN consists of the FQDN, followed by the `@` symbol, followed by the realm.

For example, the SPN for a device named swi-sem located at <http://www.yourcompany.com> would be <http://swi-sem.yourcompany.local@YOURCOMPANY.COM> where swi-sem.yourcompany.local is the FQDN, and YOURCOMPANY.COM is the realm.

1. Do the following to obtain the SEM host name and IP address:

- a. Open the SEM CMC command line.

See [Log in to the SEM CMC command line interface](#) for instructions.

- b. At the prompt, enter `appliance` to access the Appliance menu.

```

////////////////////////////////////
///      SolarWinds Security Event Manager      ///
///                               management console                               ///
////////////////////////////////////

Detected VMware Virtual Platform
Product Support Key: [REDACTED]
Available commands:
[ appliance ]  Network, System
[ manager ]   Upgrade, Debug
[ service ]   Restrictions, SSH
[ rawlogs ]   Raw logs Configuration/Maintenance
upgrade       Upgrade this Appliance
help          display this help
exit          Exit
cmc >

```

- c. At the prompt, enter `viewnetconfig`.
- d. When prompted, enter `b` to select the brief network configuration.
- e. Record the domain name, host name, and the host name's resolved IP address.
- f. Exit the management console.

2. Create a new user (host) in DNS:

- a. Open DNS manager on your domain controller.
- b. Create an `A` record entry for SEM on the DNS server using the host name and IP address. Verify that DNS Manager populated the domain field with the correct domain membership.

3. Open Active Directory Users and Computers.

4. Create an organizational unit (OU) and name it `Keytab`.

5. Select the Keytab OU and create a new user account (or Service Principle Name [SPN]).

Write down the SPN. You will need it in a later step.

6. Use the Kerberos keytab file using the `ktpass` command:
 - a. Log in to the Active Directory server as an administrator.
 - b. Open a command prompt as an administrator.
 - c. Run the following `ktpass` command:

```
ktpass -princ HTTP/<fqdn>@<REALM> -pass <SPN_account_password>  
-mapuser <domain_name>\<user_name> -pType KRB5_NT_PRINCIPAL -crypto  
ALL -out c:\sem.keytab
```

i If you receive an error when you run the command, replace the `-mapuser` argument with `-mapuser <user_name>`.

The `ktpass` command takes the following arguments:

- `-princ` specifies the server principal name (SPN) in the form `HTTP/<fqdn>@<REALM>`. You will use this path in your SEM configuration.
 - `-pass` is the SPN account password.
 - `-mapuser` maps the Kerberos principle name (specified in the `-princ` argument) to the specified domain account.
 - `-pType` specifies the principal type as Kerberos 5 for Microsoft Windows.
 - `-crypto` specifies the encryption type. Entering `ALL` indicates all supported types.
 - `-out` specifies the name and location for the generated Kerberos 5 keytab file.
7. Navigate to the keytab file location (for example, `c:\sem.keytab` specified in the `-out` argument).
 8. To allow SEM access to Active Directory, import the keytab file into SEM.

Configure SSO settings

SEM 2021.2 and later simplifies and improves Single Sign-On (SSO) configuration, moving these to the Authentication section of Settings.

i SEM uses HTTP/2 protocols and rejects HTTP/1 requests. However, if you use Single Sign-On, HTTP/1 has to be enabled as SSO uses Kerberos/NTLM authentication which does not support HTTP/2. If SSO is subsequently disabled, HTTP/1 is also disabled.

1. To view the Authentication section, click  and select Authentication.
2. Select the SSO Configuration tab.

AUTHENTICATION	LOGIN OPTIONS	LOCAL USERS	LDAP CONFIGURATION	SSO CONFIGURATION
EVENTS LIMITS	+ Create configuration 🔄 Reload data			
IMPROVEMENT PROGRAM	↑ Name ↓ Search... 🔍			
LOG FORWARDING	✓ ☒ HTTP/jenda-sem.pro.test@PRO.TEST ⋮			
MANAGE LICENSE	✓ ☒ HTTP/sem-ipotap-local.jmik.local@JMIK.local ⋮			
SECURITY	✓ ☒ HTTP/sem-sso.dh.local@DH.LOCAL ⋮			
SYSTEM RESOURCES	✓ ☒ HTTP/sem.vikings.local@VIKINGS.LOCAL ⋮			
THREAT INTELLIGENCE	✓ ☒ http/lem-recording-test.lab.exc@LAB.EXC ⋮			
UPDATES				
WEB CONSOLE				

Existing SSO Configurations are listed. These can be temporarily deactivated using the green toggle switches.

To add a new SSO login:

1. Click Create Configuration to display the Create SSO Configuration window.

Create SSO Configuration

[? Learn more about SSO](#)
[✕](#)

Service Principal Name (SPN)

Keytab file

[Browse file](#)
No file selected yet.

[Cancel](#)
[Create](#)

2. Enter the Service Principle Name (SPN). For example:
http/sem.yourcompany.local@YOURCOMPANY.COM

3. Click Browse, and then select the keytab file.

See [Generate a keytab file using Ktpass](#) for further information.

4. Click Save.

Your keytab file is uploaded to SEM. If you are logged in as a local user, SEM logs you out of the Admin user interface.

This SSO is now configured on SEM.

Edit or delete a SSO

To edit or delete a SSO, click the vertical ellipsis icon after the SSO name and click Edit or Delete.

Configure browser settings for SSO

By default, most browsers do not restrict the transmission of login credentials for intranet sites. However, your company may have policies that have this restriction on intranet sites.

Google Chrome, Microsoft Edge, and Opera

1. Click Search and enter Internet Options.

The Internet Properties window is displayed.

2. Click the Advanced tab and scroll down to the Security section.
3. Check that Enable Integrated Windows Authentication is enabled. If not, check the box.
4. Click the Security tab and select Local Intranet.
5. Click Custom Level.
6. Scroll down to the User Authentication section at the very end of the list of options.
7. Check that Automatic logon only in Intranet zone is enabled. If not, check the box.
8. Still on the Security tab, click Sites.
9. Check that all boxes are checked, then click Advanced.
10. Add your FQDN or URL as a website in the Local Intranet zone.

For example:

`https://swi-sem.yourcompany.local`

 Be sure to add the [FQDN](#) to the list of trusted sites.

11. Save your settings and close Internet Options.

12. To test your settings, close all browser windows (clear cache, if needed), and then open the SEM FQDN to confirm it is working.

Mozilla Firefox

1. Open Firefox, and then enter `about:config` in the address bar.
2. In the Filter field, enter `network.negotiate-auth.trusted-uris`.
3. In the list, double-click `network.negotiate-auth.trusted-uris`.
4. Enter the fully-qualified domain name (FQDN) or URL that you use for SEM.

For example: `mysemappliance.example.com`

The web browser is now configured for SSO.

Configure SEM for either SSO-only authentication, or SSO and local authentication

Complete these steps to configure which credentials users can use to log in to SEM. You can allow users to log in with either local SEM credentials or SSO (LDAP) credentials, or you can restrict users to only SSO (LDAP) credentials.

1. Select the Login Options tab.

AUTHENTICATION	LOGIN OPTIONS	LOCAL USERS	LDAP CONFIGURATION	SSO CONFIGURATION
EVENTS LIMITS	LOCAL USERS			
IMPROVEMENT PROGRAM	Local users authentication allows users created in SEM appliance to log into web UI and SEM Reports with set credentials. This option can only be turned off if there is a proper LDAP configuration created. Learn more			
LOG FORWARDING	☒ Allow local users authentication			
MANAGE LICENSE	SSO AUTHENTICATION			
SECURITY	SSO only authentication disables authentication into web UI using LDAP credentials and local users credentials. Learn more			
SYSTEM RESOURCES	☐ SSO only authentication			
THREAT INTELLIGENCE				
UPDATES				
WEB CONSOLE				

2. Use the toggle switches to select the login options to be used.

Updates take place immediately. Log in using the appropriate credentials to verify that the settings are correct.

Configure SSO settings in SEM using the command-line

 This option is deprecated in versions 6.8 and later.

Use these alternate steps if you do not want to use the SEM admin user interface to upload the keytab file. (You do not have to repeat this process if you already uploaded the keytab file to SEM.)

1. Log in to the CMC command-line interface.

See [Log in to the SEM CMC command line interface](#) for instructions.

2. At the `cmc>` prompt, enter `import`.

```
////////////////////////////////////  
///      SolarWinds Security Event Manager      ///  
///              management console              ///  
////////////////////////////////////  
  
Detected VMware Virtual Platform  
Product Support Key: 1-800-425-2639  
Available commands:  
[ appliance ] Network, System  
[ manager ]   Upgrade, Debug  
[ service ]   Restrictions, SSH  
[ rawlogs ]   Raw logs Configuration/Maintenance  
upgrade      Upgrade this Appliance  
help         display this help  
exit         Exit  
cmc > █
```

3. Follow the prompts on your screen to complete the import.

The file is uploaded in the appliance file system.

4. Return to the management console menu.
5. At the `cmc>` prompt, enter `admin` to access the admin command-line interface.
6. Enter your user name and password.

```

Configuration Management
* Settings
Log in Using SSO
  Console browser cannot be used for SSO authentication.
Log in Using Credentials
  * Username admin
  * Password *****
  * LOGIN

LEM 6.3.0  2008-2016 SolarWinds Worldwide, LLC. All Rights Reserved.

Data transfer complete
  Enter text into the field by typing on the keyboard
  Ctrl-U to delete all text in field, [Backspace] to delete a character
  
```

7. Arrow down to LOGIN, and then press Enter.
8. Arrow down to SSO configuration, and then press Enter.

```

<<< Configuration Management
* Settings
* admin (LOGOUT)

Settings
Authentication
  * SSO Configuration Manage Single Sign On (SSO) connection settings. At
    least one LDAP connection must be configured to enable SSO.
  * LDAP Configuration Manage LDAP connection settings.
  * Local Users Enable/disable (LEM system only) users.

LEM 6.3.0  2008-2016 SolarWinds Worldwide, LLC. All Rights Reserved.

Data transfer complete
  Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
  H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
  
```

9. Arrow down to Add New Configuration, and then press Enter.

 The content on this screen may vary with your SEM implementation.

```

<<< Configuration Management
* Settings
* admin (LOGOUT)

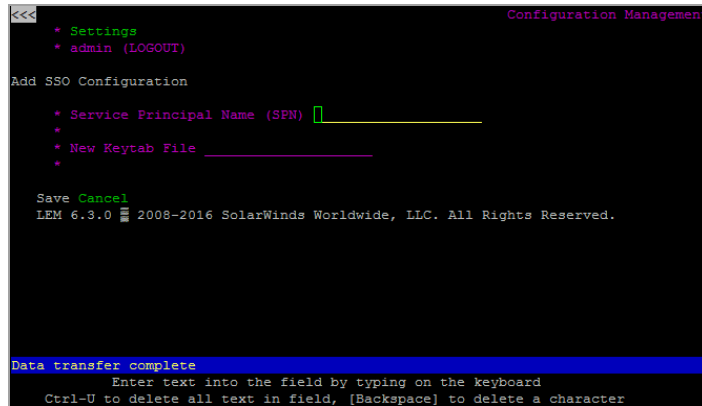
SSO Configuration Management

Text-based web browsers do not support SSO authentication. If you set
authentication to SSO only, you cannot log in using this interface.
You must log in using a supported web browser.
* Enabled authentications [Credentials and SSO] Save
*

Service Principal Name
Disable HTTP/alpha.lemsec.lab@LEMSEC.LAB Edit DELETE
Add New Configuration
LEM 6.3.0  2008-2016 SolarWinds Worldwide, LLC. All Rights Reserved.

Data transfer complete
  Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
  H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
  
```

10. Enter your SSO configuration settings.



- Enter the Service Principle Name (SPN). See [Generate a keytab file using Ktpass](#) for details.

For example: `http/swi-sem.yourcompany.local@YOURCOMPANY.COM`

- Enter the path to your keytab file using the following syntax:

`/var/transfer/storage/<your_keytab_file_name>.keytab`

11. Arrow down to Save, and then press Enter.

The upload is completed.

12. Exit the management console.

SSO is now configured on your appliance.

Updates take place immediately. Log in using the appropriate credentials to verify that the settings are correct.

Change the SEM CMC password

The CMC command-line interface (CLI) is used to connect to the SEM VM and perform administrative tasks. SolarWinds recommends that you periodically change the password used to access the CMC command-line.

 These steps require the current CMC password. The default password is `password`.

- Log in to the CMC command-line interface.

See [Log in to the SEM CMC command line interface](#) for instructions.

- Type `appliance`, and then press Enter.

- Type `password`, and then press Enter.

4. Complete the wizard to change the password. See [Special characters allowed in CMC commands and passwords](#) for help choosing a CMC password.
5. To return to the root CMC command line, type `exit`, and then press Enter.
6. To log out and close the CMC interface, type `exit`, and then press Enter again.

Test the new CMC password by logging back in to the CMC interface.

Recover a lost CMC password

You need a valid CMC password to change the password. If you no longer have a CMC password to log in to the CMC interface, contact SolarWinds Support. A support representative can help you reset the password.

You can still access the CMC interface without the CMC password by logging into the VM console through the hypervisor and clicking on Advanced Configuration.

Monitor role users and filters

SEM users assigned to the Monitor role can access their assigned filters, but cannot create, edit, delete, or import/export filters.

 See [About SEM roles](#) for more information.

By default, this role can access the same filter set as other user roles. To remove or modify the filters that Monitor users can access in the console, complete the following steps. Some steps must be completed on the end user computer. When the user logs in to SEM using the same computer and Windows profile, they can access the filters assigned to them by an administrator.

1. Log in to the SEM Console as an administrator.
2. In the toolbar, click Configure > Users.
3. Select the checkbox next to the targeted user and click Edit User.
4. In the Edit user window, click the Role drop-down menu, temporarily assign the user to the Administrator role, and then click Save.
5. Instruct the user to log in to the SEM console using their Windows profile.
6. Change the filters as needed, deleting any unnecessary filters.

 If you created and exported the filters in a previous procedure, you can add new filters to the user Filters list by creating or importing the filter as appropriate. To remove a filter from the user Filter list, point to the filter and click x that appears to the right.

7. Instruct the user to log out and close the SEM Console.
8. In the SEM Console, click Edit user for the targeted user.
9. Click the Role drop-down menu, select Monitor, and then click Save.
10. Instruct the user to log in to the SEM Console with their user credentials, and then click Monitor.

The user should only see the specified filters.

Collect event data from systems and devices

This section describes how to configure SEM to collect event data from systems, devices, and applications in your IT environment. SEM can receive events sent by SEM agents, syslog, and SNMP.

i SEM can correlate SNMP traps from devices and applications that have a corresponding connector. To configure SEM to receive SNMP traps, turn on the SNMP Trap Logging Service. See [Enable SEM to receive SNMP traps](#) for details.

About SEM Manager and agent communications

Beginning with version 2023.2, SEM implements several updates to ensure uninterrupted communications between the SEM Manager and agents. These updates include:

- [New certificates](#)
- [Agent certificate recovery](#)
- [Automatic certificate updates](#)
- [Endpoint identification](#)

New certificates

SEM Manager implements a new communication certificate that links with a new SEM agent certificate on each end-entity device. SEM Manager will support the existing SEM agent certificate until each agent has the new certificate. All SEM agent certificates are updated when the agent connects with SEM Manager.

See [Prepare to upgrade SEM](#) for instructions on how to upgrade your deployment with the latest certificates.

i The 2022.4.1 and earlier local and remote agent installer is not compatible with the SEM 2024.2.1 release.

Agent certificate recovery

When an agent attempts to connect to the SEM Manager and an error occurs (for example, the SEM agent certificate is expired), the agent automatically attempts to recover.

Automatic certificate updates

The SEM Manager and agents automatically update expired or nearly expired certificates in the background. The certificate update procedure occurs once a day by default when the SEM agent or manager is active and after the agent or manager is restarted.

SEM uses validity offsets to verify the expiration date for CA and end-entity certificates. This process helps to prevent expired certificates that can impact your SEM operations. The following table describes the offset for each certificate type.

Certificate	Default validity offset	Description
CA	One year	Certificates valid for five years are considered expired when their validation term diminishes to one year or less.
End-entity (SEM Manager and agents)	30 days	Certificates valid for 90 days are considered expired when their validation term diminishes to 30 days or less.

SEM Manager certificates

The SEM Manager end-entity certificate is always reissued after each restart and during the hostname change operation (CMC).

The background update job updates the end-entity certificate by issuing the certificate with the current CA. The existing end-entity certificate is replaced by the new certificate.

This update job also creates a new CA that includes a new end end-entity certificate. The existing (old) CA and entity certificate are saved to allow the existing agents to connect with the SEM Manager. These certificates are removed after all agents update their certificates with the certificate issued by the CA. This process starts a new CA certificate notification and broadcast job in the SEM Manager.

New CA certificate notifications and broadcasts

When the SEM Manager generates a new CA certificate, it starts a periodical background job. This job is canceled when all online SEM agents begin using a new communication certificate signed by the new CA.

Agent certificates

The background certificate update also runs on the SEM agents. When the certificate update job recognizes that the agent certificate requires an update, the agent asks the SEM Manager to issue a new certificate.

The existing agent certificates are updated after your SEM agent is upgraded to version 2023.2. After the SEM Manager updates the SEM agent certificates, the existing certificates are deleted.

Certificate update audits

The SEM Manager audits the certificate operations, including certificate updates and SEM agent certificate signing. The audit information can help you identify certificates and troubleshoot any SEM operation issues.

SolarWinds recommends [creating a filter](#) to manage the certificate update process. Below is an example of the parameters you can use to create a certificate audit filter and manage the certificate update process.

Name

Com certificate

Filter is true when

Any Alert.ProviderSID is equal to com-certificate

OR

InternalAgentOnline occurred

OR

InternalAgentOffline occurred

Click or drag item from the left panel.

where `Any Alert.ProviderSID` is the security identifier (SID) of your targeted alert provider.

Below is an example of the audit results for a CA certificate update.

Event Type	InternalAuditSuccess
EventInfo	Updated communication CA certificate
DetectionIP	
ToolAlias	auditing
ProviderSID	com-certificate
Severity	2
InsertionTime	2023-02-08 17:33:40
Manager	
InsertionIP	
DetectionTime	2023-02-08 17:33:40
ExtraneousInfo	old: <empty>; new: serial=' ' subjectDn='C=US, O=SolarWinds Inc., OU=Security Event Manager, CN=SEM Communications CA' san: <empty>
ManagerTime	2023-02-08 17:33:51

Endpoint identification

To prevent unauthorized access to your deployment, the SEM Manager and agents implement the following communications method:

1. The SEM agent connects to the SEM Manager using the manager IP or hostname (or FQDN).
2. The SEM Manager implements a TLS connection with the SEM agent and presents its certificate to the agent, which includes a list of SAN names.
3. The SEM agent compares the SEM Manager IP address from the socket against the value presented in the manager certificate SAN names. If a match exists, the connection is established. If a match does not exist, the connection fails.

Get started adding systems and devices to SEM

This section describes how to add agent devices (servers, domain controllers, and workstations), and non-agent devices (firewalls, router, and switches) to SEM.

There are two ways to configure computers and devices on your network to send log events to SEM:

- To add **servers, domain controllers, and workstations**, install a SEM agent.
- To add **firewalls, routers, or switches**, configure your devices to send log events directly to the SEM VM using syslog or SNMP traps. After configuring your device to log to SEM, configure the appropriate connectors directly on the SEM Manager.

About the SEM agent

Install the SEM agent on servers, domain controllers, and workstations to monitor local events on the systems in your network. The SEM agent is a stand-alone service that collects and normalizes log data on the remote system before it is sent to SEM for processing.

 See [Install the SEM agent](#) in the SEM Installation and Upgrade Guide for installation steps.

SEM agents can:

- Capture events in real time
- Encrypt and compress the data for efficient and secure transmission to SEM
- Buffer the events locally if the Agent loses network connectivity to SEM

In addition to monitoring local events, the agent provides event alerting on workstations and servers. It is also required for some active responses, including logging off a user, shutting down a computer, and detaching a USB device.

Install the SEM agent on computers that allow third-party software, including servers, domain controllers, and workstations. On Windows, the SEM agent captures log information from sources such as Windows Event Logs, a variety of database logs, and local anti-virus logs.

 SolarWinds recommends installing the SEM agent if you have the option. **If installing the SEM agent is not feasible, send log events directly to SEM.**

About sending log events directly to SEM

Configure non-agent devices, such as firewalls, routers, or switches, to send log events directly to SEM using syslog or SNMP traps. When you are finished, configure the appropriate device connector using the SEM console.

See [SEM connectors](#) for a list of all supported devices.

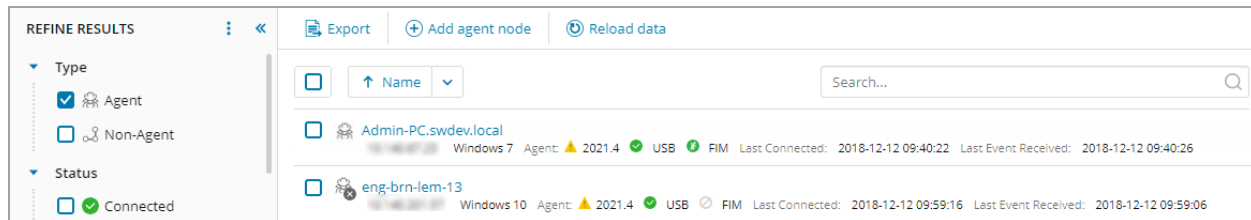
 See [Add syslog and agent nodes to SEM](#) for more information about configuring devices that do not allow third-party software.

Configure SEM agents after the installation

After you complete the installation, the SEM agent captures log information from sources such as Windows Event Logs, database logs, and local antivirus logs. Additionally, the SEM agent allows SEM to take specific actions that you can define as rules.

View the SEM Agents

1. On the SEM console, navigate to Configure > Nodes.
2. Under Refine Results, expand the Type group, and then select the Agent check box.



About the SEM Agent for Windows connectors

The SEM agent for Windows includes several preconfigured connectors that collect and display data from these systems immediately after you install the SEM Agent. By default, the SEM Agent for Windows includes the following preconfigured connectors:

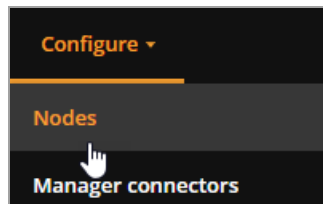
- Windows Security Log (for the host OS version)
- Windows Active Response
- Windows Application Log
- Windows System Log

For broader coverage on your Windows computers, configure specific connectors to obtain your targeted data.

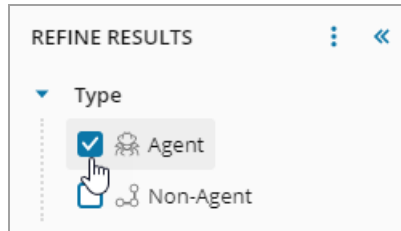
Configure the SEM agent

Perform the following steps to configure your SEM agent with one or more SEM connectors.

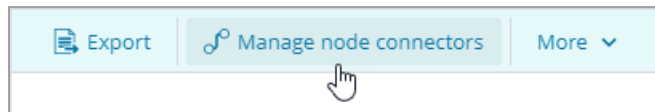
1. [Identify a SEM connector](#) for the targeted agent.
2. Log in to the SEM Console.
3. On the toolbar, click Configure > Nodes.



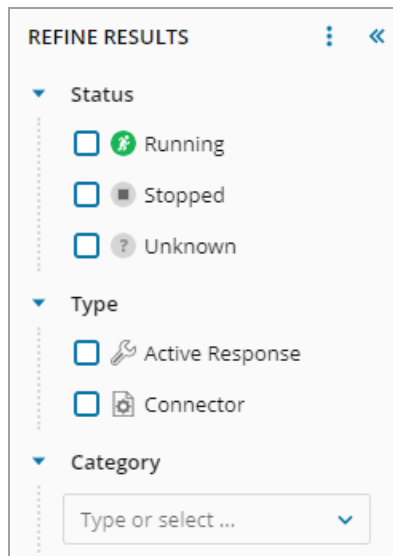
4. In the Refine Results column, expand Type and select the Agent checkbox.



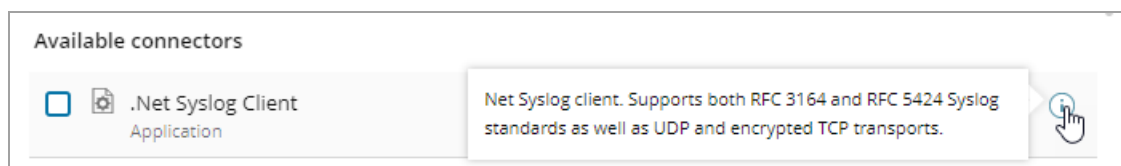
5. Select an agent, and then click Manage node connectors.



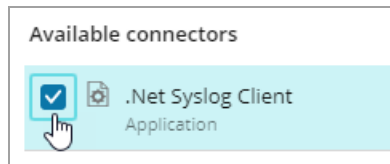
6. In the Refine Results column, sort the list of available connectors by status, type or category.



7. Under Available connectors, locate the targeted connector. Click the tooltip for a description.



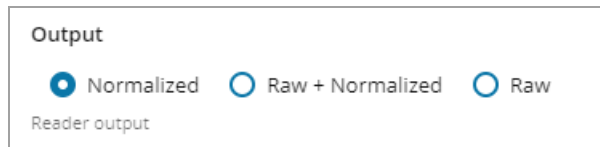
8. Select the connector checkbox.



9. In the toolbar, click Add Connector.



10. In the Add Connector window, select the output type. Configure these values if SEM is configured to save raw (unnormalized) log messages.



Select Normalized to save normalized log messages.

Select Raw + Normalized to save unnormalized and normalized log messages.

Select Raw to save unnormalized log messages.

11. Under Sleep time, click the up- or down-arrow to adjust the number of seconds between log reads (if required).



12. Click Save.

Your changes are saved to the connector profile. The connector is added to the Configured connectors list.

13. (Optional) Repeat step 7 through step 12 to add additional connectors to the agent.

14. Click Done.

The new connector displays in the Nodes with all available agents and non-agents based on your Refine Results selection.

 See [Manage the monitored nodes](#) for details on how to refine the node results, edit a connector profile, edit an active response connector profile, and more.

Create connector profiles to manage and monitor SEM agents

Use a connector profile to group agents that share the same connector configuration. You can use the profile to configure a set of standardized connector settings, and then apply those settings to all agents assigned to that profile. Once applied, every agent in the profile will have the same connector settings.

Connector profiles maintain all agents in a profile by updating only the profile connector configuration. The system then propagates your changes to all the agents in the profile.

Most agents in a network have only a few different connector configurations. Using connector profiles, you can streamline the process of connecting your network security products to SEM. If you decide not to use connector profiles, you must create at least one connector instance for every product that you intend to integrate with SEM, and then repeat this process for each agent.

A well-planned set of connector profiles provides you with a versatile and efficient method for configuring and maintaining your agent connector configurations. You can create as many connector profiles as you need to reflect each of your common connector configurations. For example, you can set up a standard user workstation profile, a web server profile, and so on. SolarWinds provides several default connector profiles that address common configurations.

About the connector-profile group type

SEM lets you use connector profiles in filters, rules, and searches. After you define a connector profile, you can use it in rules and filters to include or exclude the agents associated with that profile. For example, you can create a filter using the Domain Controller connector-profile group to show you web traffic from the computers in that group.

 Groups organize related elements for use with SEM rules and filters. See [About SEM groups](#) for information about the various SEM group types.

Connector profile guidelines

A well-planned set of connector profiles provides you with a versatile and efficient method of updating and maintaining your agent connector configurations.

When you configure your connector profiles, use the following guidelines:

- An agent can only be a member of one connector profile.
- You cannot add an agent to multiple connector profiles.

Create a connector profile: process overview

This section provides an overview of the steps required to create a connector profile. Creating a connector profile is a three-step process:

1. Install the SEM agent software on all the systems that you want to include in your new connector profile, then configure a single SEM agent to serve as the template for your connector profile.
2. Add the agents to the connector profile. When completed, the system applies the template to all agents in the profile.
3. Verify the connector status.

When you select an agent for a template, ensure the agent has a configuration that mirrors your concept of the final connector configuration.

You can prepare a template agent in advance by configuring an agent you know will be a member of the new profile. When completed, use the agent as the template for the new profile. This process minimizes your need to edit the profile connector configuration in the future.

Create a new connector profile

Create a new connector profile without preconfigured connectors or agents.

1. On the SEM Console, navigate to Configure > Connector Profiles.



2. On the Connector Profile toolbar, click Create Connector Profile, select New profile, and then click Continue.

Choose an option of how to create Connector profile



New profile

Create new profile without preconfigured connectors or agents.



From template

Create profile from a template with preconfigured connectors.



From agent

Create profile with preconfigured connectors from the selected agent.

[Cancel](#)
[Continue](#)

3. Enter a name for the profile and a description (optional), and then click Create and Next.

Create new connector profile

Profile details

Configured connectors

Assigned agents

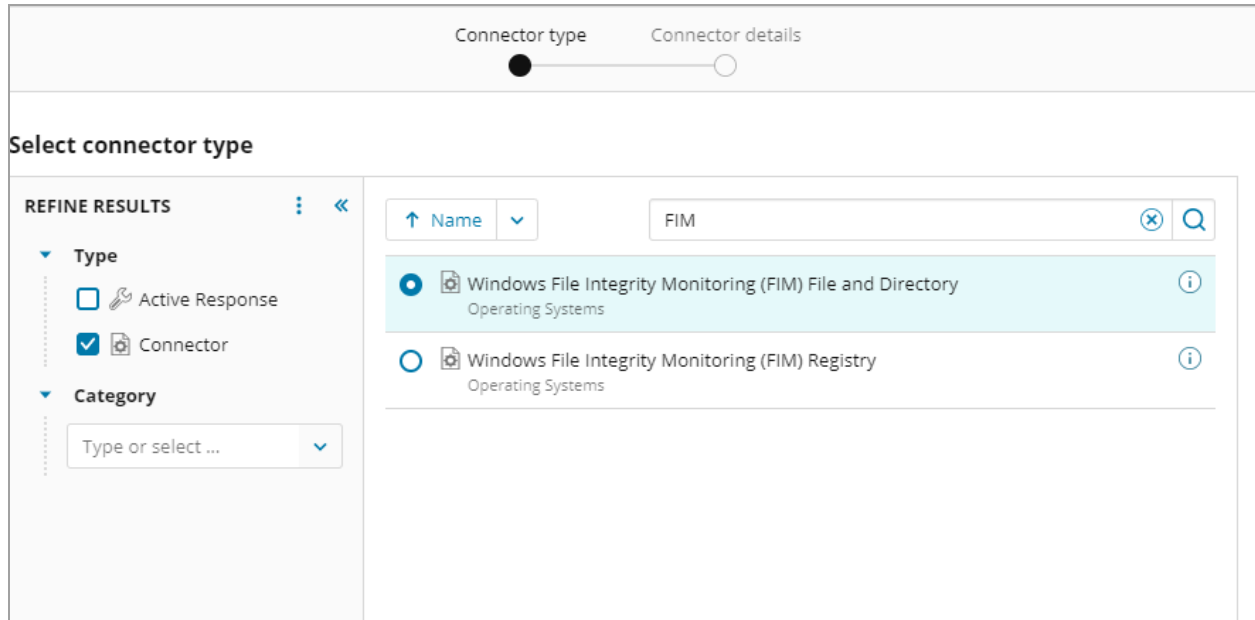
Connector profile details

Connector profile name

Description (optional)

4. Under Configured connectors, click Add connector.
5. Under Refine Results, expand the Type group, and then select Connector or Active Response (or both).

6. Find the connector to configure. Type part of the connector name in the search box, or use the filter menus in the Refine Results pane.



The screenshot shows the 'Select connector type' interface. At the top, there are two tabs: 'Connector type' (selected) and 'Connector details'. Below the tabs is a search bar with the text 'FIM'. To the left of the search bar is a 'REFINE RESULTS' pane. This pane has two sections: 'Type' and 'Category'. Under 'Type', there are two options: 'Active Response' (unchecked) and 'Connector' (checked). Under 'Category', there is a dropdown menu with the text 'Type or select ...'. The search results show two connectors: 'Windows File Integrity Monitoring (FIM) File and Directory' (selected) and 'Windows File Integrity Monitoring (FIM) Registry'. Both connectors are categorized under 'Operating Systems'.

7. Complete the connector configuration form. The following fields are common across most connectors:
 - Name: Enter a user-friendly label for your connectors.
 - Log File: Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the SEM appliance (non-Agent devices).
 - Output: Normalized, Raw + Normalized, Raw. You only need to configure these values if SEM is configured to save raw (unnormalized) log messages.
8. Click Add.
9. Add additional connectors to the profile as required, and then click Next.
10. Click Assign agents.
11. Filter and select one or more agents to add to the profile, and then click Assign.



An agent can only be a member of one connector profile. Learn more about connector profiles [here](#).

12. To complete the connector profile configuration, click Finish.

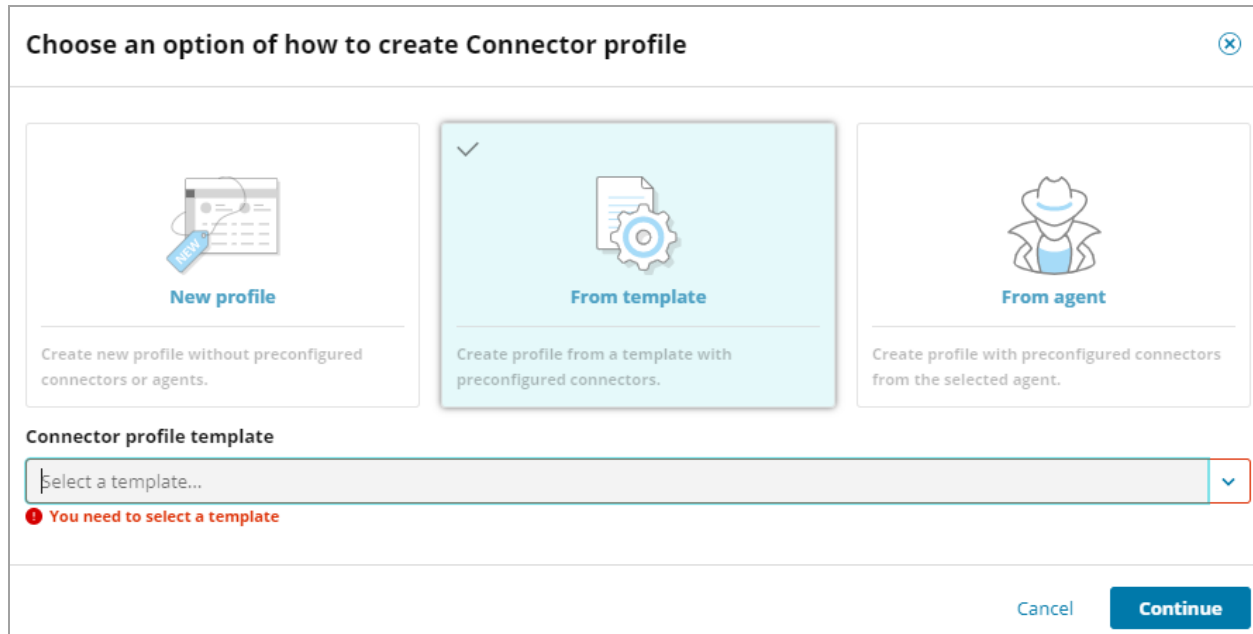
Create a connector profile from a template

Create a profile from a template with preconfigured connectors.

1. On the SEM Console, navigate to Configure > Connector Profiles.

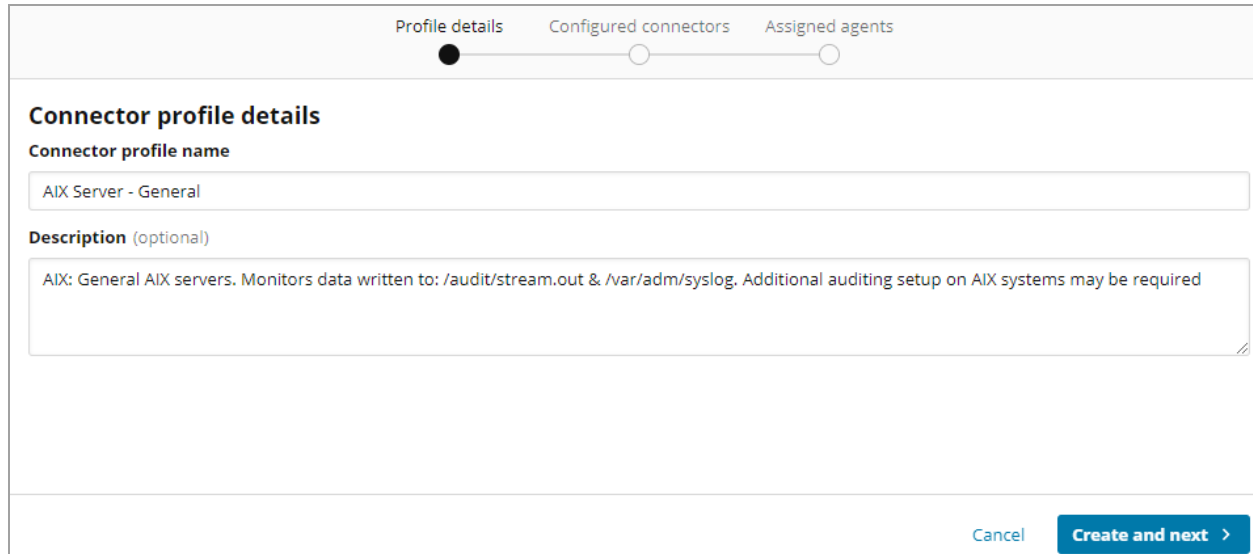


2. On the Connector Profile toolbar, click Create, and then select From template.



3. From the Connector profile template drop-down list, select a template, and then click Continue.

4. Enter a new name and description for the profile, and then click Create and Next.



Profile details Configured connectors Assigned agents

Connector profile details

Connector profile name

AIX Server - General

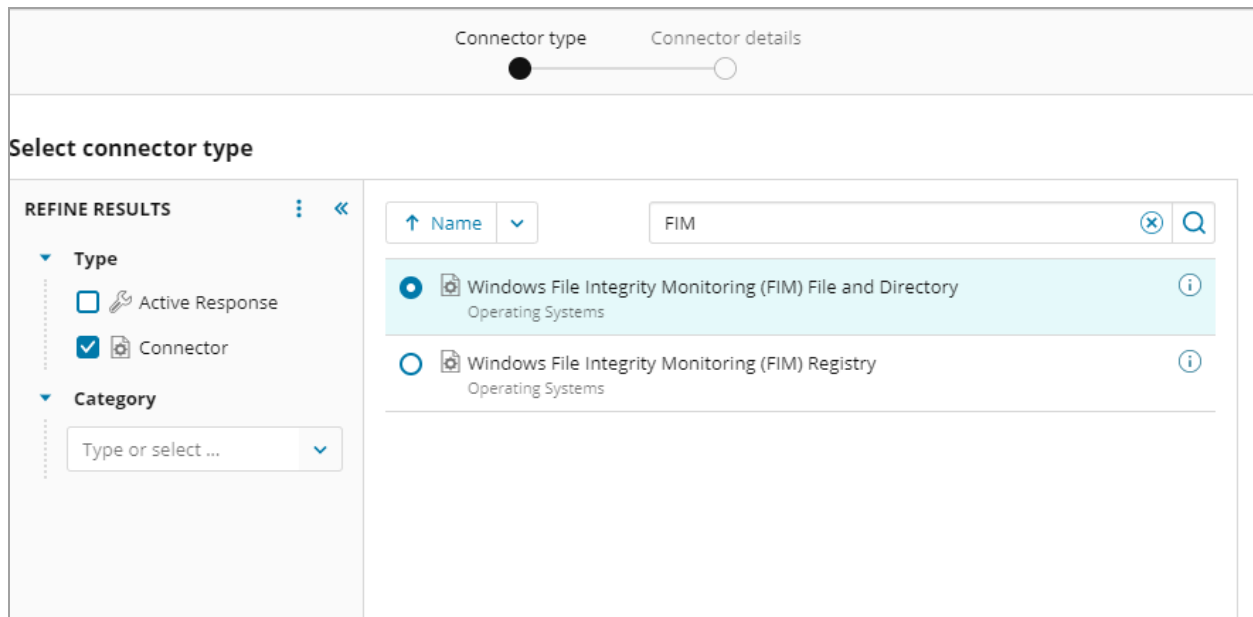
Description (optional)

AIX: General AIX servers. Monitors data written to: /audit/stream.out & /var/adm/syslog. Additional auditing setup on AIX systems may be required

Cancel **Create and next >**

Under Configured connectors is a list of preconfigured template connectors.

5. To configure an additional connector, click Add connector.
6. Under Refine Results, expand the Type group, and then select Connector or Active Response.
7. Find the connector to configure. Type part of the connector name in the search box, or use the filter menus in the Refine Results pane.



Connector type Connector details

Select connector type

REFINE RESULTS

Type

☐ Active Response

☒ Connector

Category

Type or select ...

↑ Name FIM

- ☒ Windows File Integrity Monitoring (FIM) File and Directory
Operating Systems
- ☐ Windows File Integrity Monitoring (FIM) Registry
Operating Systems

8. Complete the connector configuration form. The following fields are common across most connectors:
 - Name: Enter a user-friendly label for your connectors.
 - Log File: Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the SEM appliance (non-Agent devices).
 - Output: Normalized, Raw + Normalized, Raw. You only need to configure these values if SEM is configured to save raw (unnormalized) log messages.
9. Click Add.
10. Continue to add more connectors to the profile as needed, and then click Next.
11. Click Assign agents to add one or more agents to the profile.



An agent can only be a member of one connector profile. Learn more about connector profiles [here](#).

12. To complete the connector profile configuration, click Finish.

Create a connector profile from an agent

Create a new connector profile with preconfigured connectors from a selected agent.

1. On the SEM Console, navigate to Configure > Connector Profiles.



- On the Connector Profile toolbar, click Create, and then select From agent.

Choose an option of how to create Connector profile



New profile

Create new profile without preconfigured connectors or agents.



From template

Create profile from a template with preconfigured connectors.



From agent

Create profile with preconfigured connectors from the selected agent.

Use agent node

[Select agent node](#)

Cancel
Continue

- Click select agent node, to view a list of available agents.
- Choose an agent node from the list, click Select, and then click Continue.
- Enter a name for the profile and a description (optional), and then click Create and Next.

Profile details
Configured connectors
Assigned agents

Connector profile details

Connector profile name

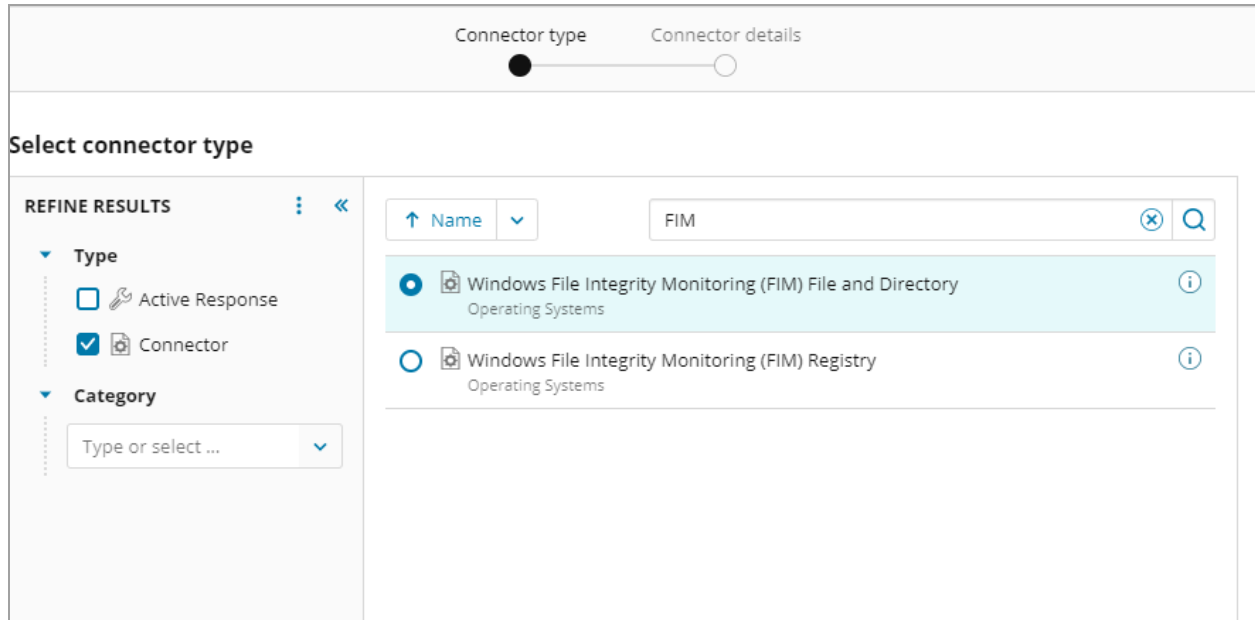
Description (optional)

Cancel
Create and next >

 Connectors that were already configured for this agent node will appear in the connector list

- Under Configured connectors, click Add connector.
- Under Refine Results, expand the Type group, and then select Connector or Active Response.

8. Find the connector to configure. Type part of the connector name in the search box, or use the filter menus in the Refine Results pane.



9. Complete the connector configuration form. The following fields are common across most connectors:
 - Name: Enter a user-friendly label for your connectors.
 - Log File: Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the SEM appliance (non-Agent devices).
 - Output: Normalized, Raw + Normalized, Raw. You only need to configure these values if SEM is configured to save raw (unnormalized) log messages.
10. Click Add.
11. Continue to add more connectors to the profile as needed, and then click Next.
12. Click Assign agents.



An agent can only be a member of one connector profile. Learn more about connector profiles [here](#).

13. To complete the connector profile configuration, click Finish.

Clone a connector profile

Cloning a connector profile allows you to duplicate an existing profile, and then make additional edits where needed. This option saves valuable time when associating new connectors and agents to a similar profile configuration.

1. On the SEM Console, navigate to Configure > Connector Profiles.
2. From the profile list, select the required connector profile, and click Clone.
3. Enter a new profile name, and then click Create.
4. Find and select your cloned connector profile in the list, and click Edit.
5. Make changes to the profile where needed, and click Finish.

Edit a connector profile

1. On the SEM Console, navigate to Configure > Connector Profiles.
2. From the profile list, select a connector profile, and click Edit.
3. Make changes to the profile as needed, and click Finish.

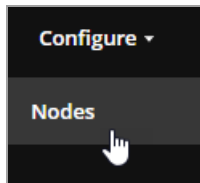
Add syslog and agent nodes to SEM

You can add syslog and agent nodes to SEM using the [SEM Console](#) and the [Getting Started wizard](#).

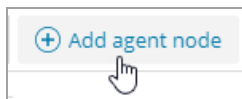
Add an agent node using the SEM Console

Use the SEM console to download a Linux agent installer. When you are finished

1. Log in to the SEM Console
2. In the toolbar, click Configure > Nodes.



3. In the toolbar, click Add agent node.



4. Download the required installer(s).

Add agent node

To install the appropriate agent for your device, download the agent for either remote or local installation.

A) Remote Installation (only for Windows)
You can directly download the [Windows Agent Remote Installer](#).

B) Local Installation
Log on to the device you want to install the agent on, then download and install the appropriate agent from the following:

- [AIX Agent Installer](#)
- [HP UX Itanium Agent Installer](#)
- [Linux 64 Agent Installer](#)
- [Linux Agent Installer](#)
- [Mac OS Agent Installer](#)
- [Solaris Agent Installer](#)
- [Solaris Intel AgentInstaller](#)
- [Windows Agent Installer](#)

After running the agent installer, you should see the events for your agent device appear in the Monitor window.

Done

- (Remote Windows installation only) Click Windows Remote Agent Installer to download the installer to your system.
- Under Local Installation, click the agent installer that matches the operating system running on the targeted device.

For example, if your targeted device is running Linux, click Linux Agent Installer.

- Click Done.
- Install the agent on a [remote Windows system](#) or a [local](#) system.

Install the agent on a remote Windows system

See [Run the SEM remote agent installer](#) to install the SEM agent on one or more remote Windows computers without an installation wizard.

Install the agent on a local system

1. Copy the installer to your targeted local system.
2. Run the installer on the local system.

For Windows systems, see [Run the SEM local agent installer](#) for instructions.

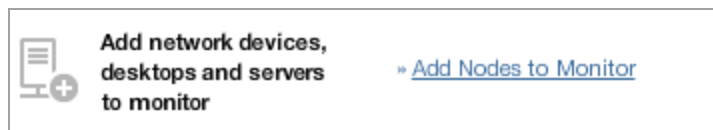
For Linux and Unix systems, see [Install the SEM agent on Linux or Unix](#) for instructions. To install on multiple servers, see [Install the Linux \(or Unix\) agent on multiple servers](#) for instructions.

For macOS systems, see [Install the SEM agent on macOS](#) for instructions.

Add an agent node using the Getting Started wizard

If you are installing SEM, you can add nodes from the Getting Started wizard.

1. In the Getting Started wizard, click Add Nodes to Monitor.



2. In the dialog box, click the drop-down menu and select an agent or non-agent node you want to add.
3. Follow the instructions on your screen to add the monitored node.

Update the SEM agents

This section describes how to update SEM agents on remote or local Windows computers.

Update SEM agents automatically

On the SEM Console Settings page, you can enable automatic updates for SEM agents and set the number of concurrent updates.

1. Log in to SEM as an administrator.
2. On the SEM Console toolbar, click the Settings icon.



3. On the Settings page, click Updates in the left column.
4. Under Agent Updates, click the toggle button to enable automatic agent updates.
5. Set the maximum number of concurrent updates, and then click Save.

 This setting determines the number of agents that can be updated at the same time.

Manually upgrade SEM agents on Unix, Linux, Mac, and Windows hosts using SEM agent installers

If you are installing SEM agents on the far end of a WAN link, copy the SEM Agent Installer executable to the end of the WAN link and run it there.

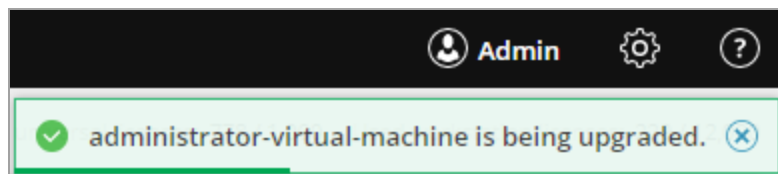
 Check the SEM release notes or readme file first to be sure that the SEM agent version you are planning to install is compatible with your installed SEM Manager version.

If you are installing SEM agents on the far end of a WAN link, copy the SEM Agent Installer executable to the end of the WAN link and run it there.

 Check the SEM release notes or readme file first to be sure that the SEM agent version you are planning to install is compatible with your installed SEM Manager version.

1. In the SEM Console, navigate to Configure > Nodes.
2. Filter nodes by selecting Type - Agent in the Refine Results column
 - To update one agent, select the agent node and select Upgrade agent from the More dropdown menu.
 - To update two or more agents, select the agent nodes and select Upgrade agent from the Commands dropdown menu.

A progress bar appears in the upper right of the console as the agents are being upgraded.



Run the SEM Remote Agent Installer for Windows

Learn how to use the SEM Remote Agent Installer [here](#).

Set up a separate syslog server for use with SEM

You can monitor your switches, routers, and firewalls using a syslog server. This server collects and sends syslog messages from non-agent devices to the SEM Manager over TCP or UDP. SEM uses this information to monitor syslog events and displays them in the [Live Events](#) and [Historical Events and Reports](#) tabs, which you can access from the toolbar.

Each device is paired with a connector, enabling SEM to parse messages from the syslog server and normalize the log message content to a SEM event.

Consider deploying [Kiwi Syslog Server \(KSS\)](#) in your deployment to act as your syslog server. KSS provides an affordable on-premises solution to manage syslog messages, SNMP traps, and Windows event logs. Otherwise, select and use an existing syslog server in your organization.

Manage the monitored nodes

The Nodes window displays two types of monitored nodes: Agents and non-agent devices. Agents are software applications installed on a monitored device. They collect and normalize log data before it is sent to the SEM Manager. Non-agent devices are hardware devices that send log data directly to the SEM Manager for normalization and processing. These devices include firewalls, switches, and routers.

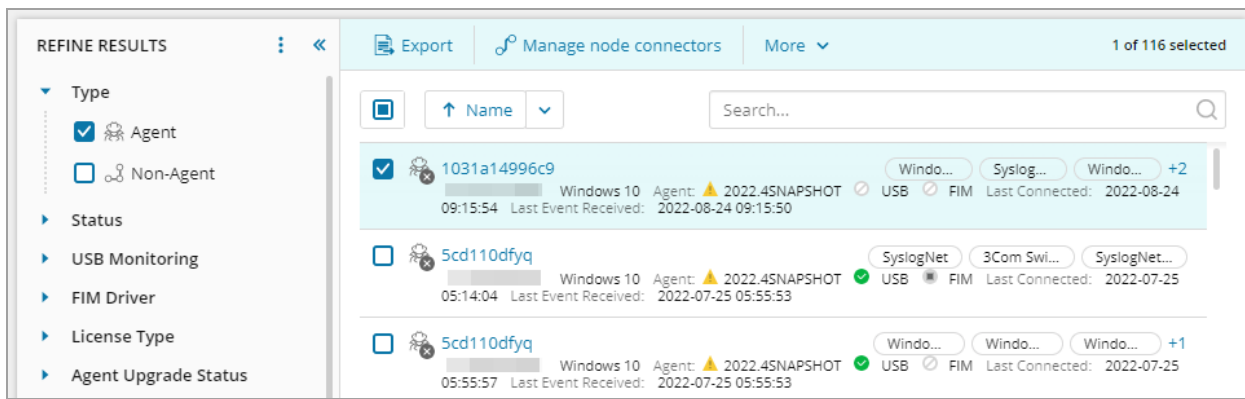
Click Configure > Nodes in the console toolbar to display your monitored nodes. If your SEM agents require an upgrade, a warning message displays on the page, as shown below.

The screenshot shows the 'Nodes' window in the SolarWinds interface. At the top, it displays license usage: 'Used universal licenses: 487 / 10,000' and 'Used workstation licenses: 12 / 1,000'. A yellow warning banner at the top left states: 'Out of date agents. There are 114 agents that should be upgraded to take advantage of the latest features and security fixes. See out of date agents'. Below the banner, the 'REFINE RESULTS' sidebar on the left lists various filters: Type, Status, USB Monitoring, FIM Driver, License Type, Agent Upgrade Status, Operating System, Connector Profiles, Last Connected, and Last Event Received. The main area shows a list of nodes with columns for selection, name, and last event received. The nodes listed are: 047-014-006-068 (Last Event Received: 2022-05-31 07:49:18), 10.110.0.51 (Last Event Received: 2022-01-27 01:30:28), 10.110.0.52 (Last Event Received: 2022-01-27 01:30:34), 10.110.60.146 (Last Event Received: 2022-04-21 03:09:00), and 10.110.60.185 (Last Event Received: 2022-04-21 03:08:55). At the bottom, there is a pagination bar showing '1-25 of 499' and a dropdown for '25'.

You can add agent nodes, configure node connectors, and monitor activity. After you configure the nodes and connectors, click Live Events in the toolbar to view your network activity. Here, you can create and apply filters to tailor your log feed, allowing you to view event logs that are detrimental to the health of your network environment.

Refine the node results

Refine the node results by selecting an option in the Refine Results column. For example, to view all monitored agents, maximize Type and select the Non-Agent checkbox. All agents display in the center console with details about each monitored agent.



The following table lists actions you can perform on the Nodes page.

If you want to...	Do the following:
Add an agent node	Deselect all options in the left column, and then click Add agent node in the toolbar.
Export the node list to a CSV file	Click Export in the toolbar.
Manage your node connectors	Select an agent type (agent or non-agent), select a connector, and then click Manage node connectors in the toolbar.
Organize your node list by IP address, operating system type, or version	Click the Name drop-down menu in the toolbar and select an option.
Locate a specific node in the node list	Enter a search parameter in the Search field.
Refresh the nodes list	Click Reload data in the toolbar.

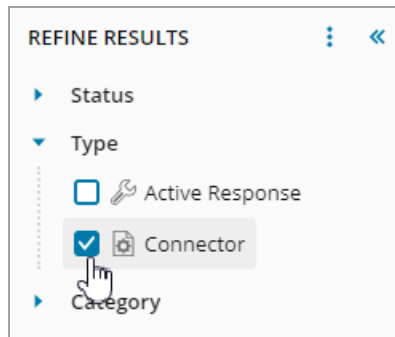
Edit a connector profile

This procedure explains how to edit a connector profile that you [created](#) to manage and monitor SEM agents.

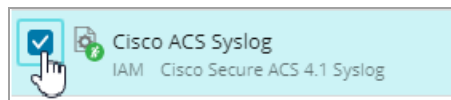
 See [Create a new connector profile](#) for instructions on how to create a connector.

1. Log in to the SEM Console as an administrator.
2. In the toolbar, click Configure > Manager connectors.

3. In the Refine Results column, maximize Type and select Connector to refine the connector list to non-active response connectors.



4. Select a connector in the list. For example:

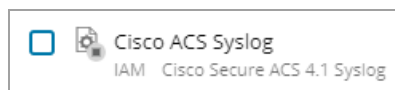


Click  to view a description of the connector.

5. Click Stop.



The green indicator next to the connector name disappears, indicating that the connector is stopped.



6. Reselect the targeted connector, and then click Edit.



7. Edit the node connector parameters as required.

- a. Update the connector name (if required).

Name
Cisco ACS Syslog
Connector name

- b. Leave the log file path intact.

Log File

/var/log/local4.log

Directory or path to read from

- c. Update the connector reader output (if required).

Output

☒ Normalized
 ☐ Raw + Normalized
 ☐ Raw

Reader output

Select Normalized to save normalized log messages.

Select Raw + Normalized to save unnormalized and normalized log messages.

Select Raw to save unnormalized log messages.

- d. Click the up- or down-arrow to adjust the number of seconds between log reads (if required).

Sleep Time

1

Number of seconds between log reads

- e. Click Save.

Your changes are saved to the connector profile.

8. Make sure the connector checkbox is selected.

☒

 Cisco ACS Syslog
 IAM Cisco Secure ACS 4.1 Syslog

9. Click Start.



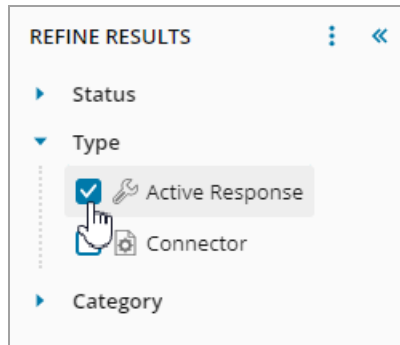
The green indicator next to the node name displays, indicating that the connector is started and running.

☐

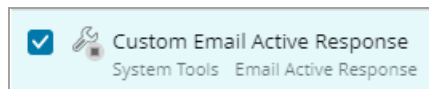
 Cisco ACS Syslog
 IAM Cisco Secure ACS 4.1 Syslog

Edit an Active Response connector

1. Log in to the SEM Console as an administrator.
2. On the toolbar, click Configure > Manager connectors.
3. In the Refine Results column, maximize Type and select Connector to refine the connector list to active response connectors.



4. Select a an active response connector in the list. For example:

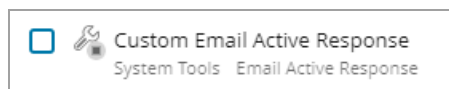


Click  to view a description of the connector.

5. Click Stop.



The green indicator next to the connector name disappears, indicating that the connector is stopped.



6. Reselect the targeted connector, and then click Edit.



7. Edit the node connector parameters as required.

- a. Update the connector name (if required).

Name
Custom Email Active Response
Connector name

- b. Verify that the mail host URL is correct. Edit if required.

Mail Host
example.com

- c. Verify that the port value is correct. Edit if required.

Port
4444

Based on the selected Transport Protocol value, this field defaults to one of the following:

- 25 (Standard, non-secure SMTP)
- 465 (SSL)
- 587 (TLS)

- d. Verify that the return address is correct. Edit if required.

Return Address
admin@example.com

- e. Verify that the return display name is correct. Edit if required.

Authentication Server Username
admin

- f. Verify that the authentication server password is correct. Edit if needed.

Authentication Server Password

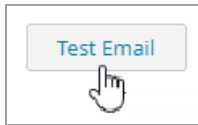


This password may not be your normal account password. See your SMTP host provider for details.

- g. Enter a test e-mail address in the field.

Test E-mail Address
user@example.com

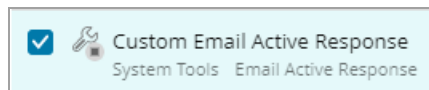
- h. Click Test Email to test.



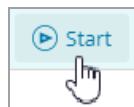
- i. Check the email message.
- j. Click Save.

Your changes are saved to the connector profile.

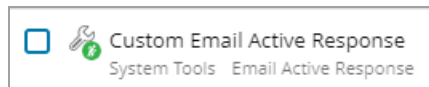
8. Make sure the connector checkbox is selected.



9. Click Start.



The green indicator next to the connector name displays, indicating that the connector is started and running.



Delete a connector

1. Log in to the SEM Console as an administrator.
2. On the toolbar, click Configure > Manager connectors.
3. Locate and select the connector you want to delete.
4. Click More > Delete.
5. Follow the prompts on your screen to complete the procedure.

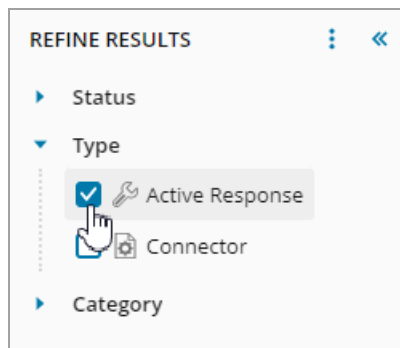
Edit an Active Response connector profile

After you create an Active Response connector during the initial setup, you can update and test the connector profile.

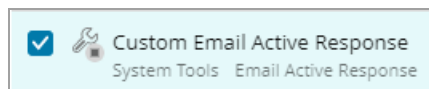
Beginning with version 2023.2, the connector profile includes a Test button that allows you to send an email through your SMTP server to a targeted user when the connector detects an issue in your deployment. This process ensures that the response email reaches the targeted user.

See [Create a new connector profile](#) for instructions on how to create a new connector profile.

1. Log in to the SEM Console as an administrator.
2. On the toolbar, click Configure > Manager connectors.
3. In the Refine Results column, maximize Type and select Connector to refine the connector list to active response connectors.



4. Select an active response connector in the list. For example:

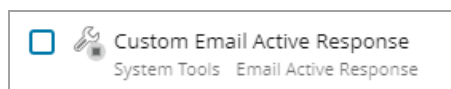


Click  to view a description of the connector.

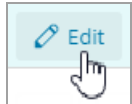
5. Click Stop.



The green indicator next to the connector name disappears, indicating that the connector is stopped.



6. Reselect the targeted connector, and then click Edit in the toolbar.



7. Edit the node connector profile as required.

- a. In the Name field, enter a new name or keep the existing name.

Name
Custom Email Active Response
Connector name

- b. In the Mail Host field, verify that the IP address or hostname is correct.

Mail Host
example.com

If you use a hostname (as shown above), SEM Manager must be able to resolve the mail host from the DNS entries you entered when you configured your SEM network.

- c. In the Transport Protocol field, verify that the selected protocol is correct. To update, click the drop-down arrow and select SMTP, SSL, or TLS.

Transport Protocol
SMTP

In this example, SMTP is selected as the transport protocol.

 TLS 1.2 is supported for email connections in SEM 2020.2.1 and later.

- d. Verify that the port value is correct.

Port
25

Based on the value you selected in the Transport Protocol field, this field defaults to one of the following ports:

- 25 (Standard, non-encrypted SMTP)
- 465 (SSL with encryption)
- 587 (TLS with encryption)

- e. In the Return Address field, verify that the return address is correct. Edit if required. For example:

Return Address
noreply@solarwinds.com

 This field is pre-populated with noreply@solarwinds.com. Be sure to change this email address to an address associated with your organization.

- f. In the Return Display Name field, verify that the return display name is correct. Edit if required. For example:

Return Display Name
SolarWinds

- g. (Optional) If the email server requires an Active Directory user to send email, enter the authentication server user name in the Authentication Server Username field.

Authentication Server Username
admin

- h. (Optional) If the email server requires an Active Directory user to send email, ensure that an authentication server password exists in the Authentication Server Password field.

Authentication Server Password

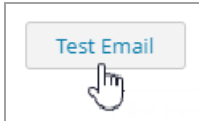
 If you are retesting the email configuration, re-enter the password.

- i. (Optional) In the Test E-mail Address field, verify that the e-mail address is correct. This address is used to verify that an e-mail can be sent to a user when generated by an active response connector. For example:

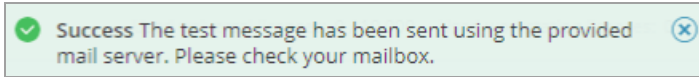
Test E-mail Address
user@example.com

 If the email server requires an email to be sent from a computer within the domain, the email server must have an exception created for the SEM hostname. SEM cannot join the domain.

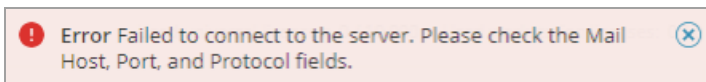
- j. (Optional) Click Test Email to test.



If the test message was sent successfully through the SMTP server, the following message displays in the console:



If the test message was not sent successfully through the SMTP server, a message displays in the console. For example:



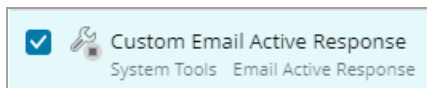
The Error test message provides details about the failure and provides suggestions to troubleshoot the failure.

 The response message may require up to 30 seconds to display in the console. If you do not receive a response, the e-mail address in the Test E-mail Address field may be incorrect or SEM cannot reach the SMTP server through your network.

- k. (Optional) Verify that the user who owns the test e-mail address received the test email.
- l. Click Save.

Your changes are saved to the connector profile.

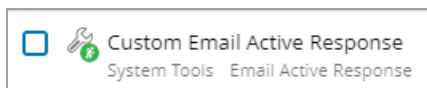
8. Make sure the connector checkbox is selected.



9. Click Start.



The green indicator next to the connector name displays, indicating that the connector is started and running.



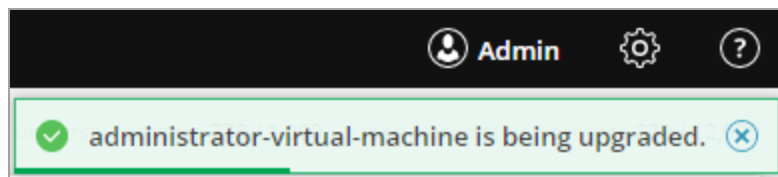
Update the SEM agents manually

If you are installing SEM agents on the far end of a WAN link, copy the SEM Agent Installer executable to the end of the WAN link and run it there.

i Check the SEM release notes or readme file first to be sure that the SEM agent version you are planning to install is compatible with your installed SEM Manager version.

1. In the SEM Console, navigate to Configure > Nodes.
2. Filter nodes by selecting Type - Agent in the Refine Results column
 - To update one agent, select the agent node and select Upgrade agent from the More dropdown menu.
 - To update two or more agents, select the agent nodes and select Upgrade agent from the Commands dropdown menu.

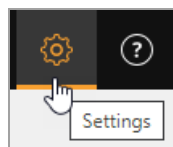
A progress bar appears in the upper right of the console as the agents are being upgraded.



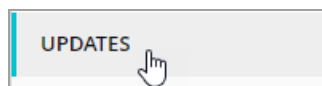
Update the SEM connectors automatically

On the SEM Console Settings page, you can enable automatic updates for SEM connectors.

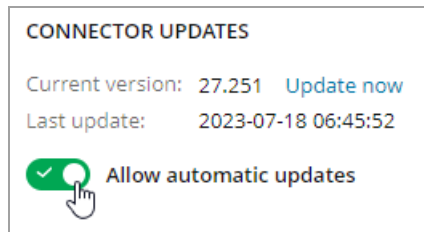
1. Ensure that the following URL is whitelisted from the SEM server in your proxy or firewall:
downloads.solarwinds.com
2. On the SEM console toolbar, click Settings.



3. On the Settings page, click the Updates tab in the left column.



4. In the Connector Updates section, click the toggle button to allow automatic updates.



5. Click Save.

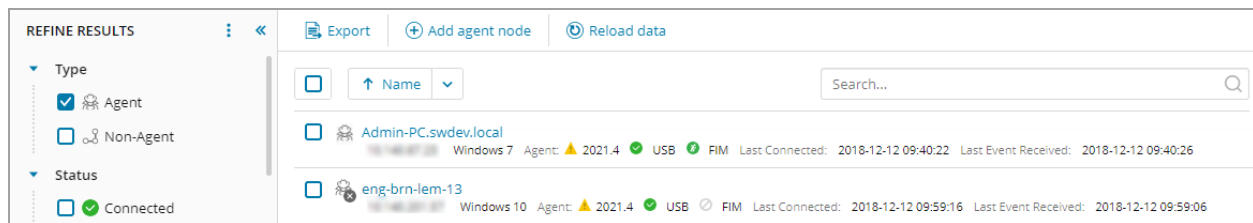
Add and remove agents from connector profiles

If required, you can add or remove an agent from a connector profile.

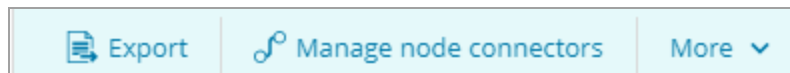
Add an agent to a profile

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. In the Refine Results column, select Agent.

 Learn more about connector profiles [here](#).

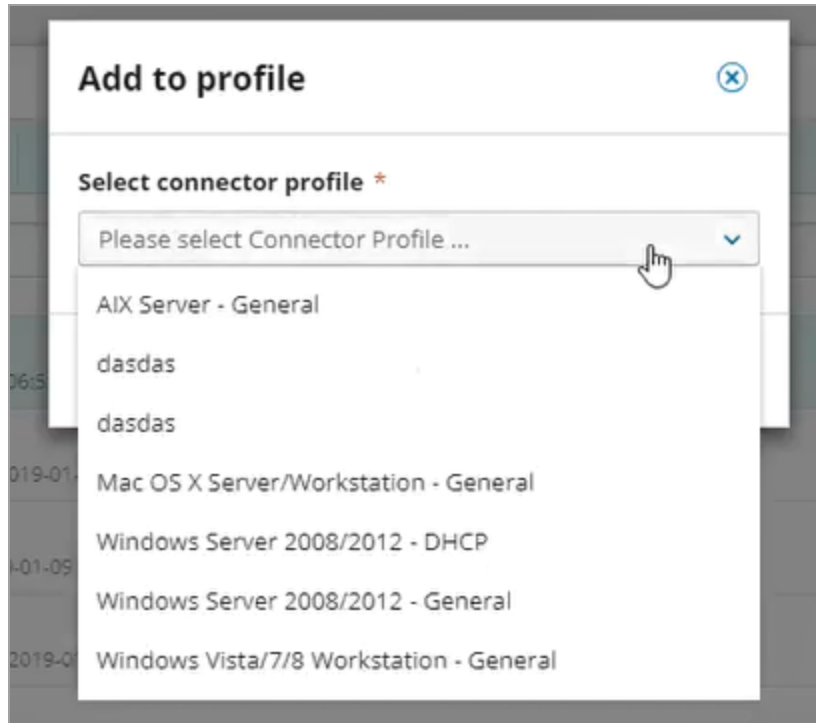


4. Select an agent check box to expose the configuration toolbar.



5. From the More drop-down list, select Add to Profile.

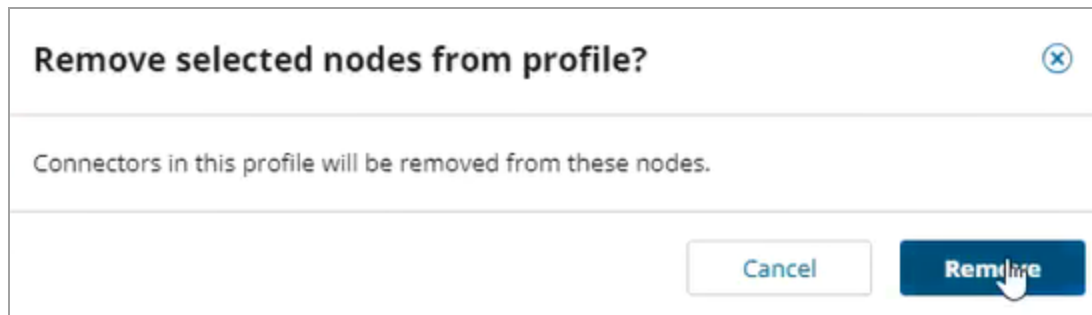
6. Select a profile from the list, and then click Add.



A notification appears indicating the agent was added successfully.

Remove an agent from a profile

1. Select an agent, and then navigate to More > Remove from Profile. A confirmation dialog appears.



2. Click Remove.

Configure Windows domain controller connectors

Configure the following connectors that apply to your installation on your Windows domain controllers:

Available connectors	
☐	Windows DHCP Server 2000 Network Services
☐	Windows DHCP Server 2000/2003/2008 Event Log(Admin) Application
☐	Windows DHCP Server 2000/2003/2008 Event Log(Operational) Application
☐	Windows DHCP Server 2000/2003/2008 System Log Network Services
☐	Windows DHCP Server 2003 And 2008 Network Services
☐	Windows DNS Server Log Operating Systems
☐	Windows Directory Service Log Operating Systems

1. On the SEM Console, navigate to Configure > Nodes.
2. Under Refine Results, expand the Type group, and then select the Agent check box.
3. Select an agent, and then click Manage node connectors.
4. Find the connector to configure. Type part of the connector name in the search box, or use the filter menus in the Refine Results pane.
5. Select an available connector, and then click Add Connector.
6. Complete the connector configuration form. The following fields are common across most connectors:
 - Name: Enter a user-friendly label for your connectors.
 - Log File: Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the SEM appliance (non-Agent devices).
 - Output: Normalized, Raw + Normalized, Raw. You only need to configure these values if SEM is configured to save raw (unnormalized) log messages.

7. Click Add.
8. To start a connector, select a configured connector, and then click Start.

Verify USB Defender is installed on a SEM agent

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. Under Refine Results, expand the Type group and select the Agent check box.
4. To determine which nodes have USB defender, in the Agent nodes list, observe the nodes with a green check icon  next to USB.

☐	 eng-aus-dpa-073	Windows Server 2016	 USB	 FIM	Last Connected: 2019-01-09 01:50:37	Last Event Received: N/A
☐	 eng-aus-sys-350	Windows Server 2019	 USB	 FIM	Last Connected: 2019-05-20 08:56:53	Last Event Received: 2019-05-20 08:56:53
☐	 eng-aus-sys-351	Windows Server 2019	 USB	 FIM	Last Connected: 2019-05-21 22:06:26	Last Event Received: 2019-05-22 09:14:21

5. If USB Defender is not installed on one or more SEM Agents, reinstall the agent and ensure that you select Install USB-Defender after you confirm the Manager Communication Settings.

Enable additional connectors to add extra log sources to SEM

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. Select an agent node, and then click Manage node connectors.
4. Under Available connectors, select a supported device or application to log.

 Enter a keyword in the search box, or use the Category drop-down list to filter connectors by category.

5. Select an available connector, and then click Add connector.
6. Update your settings, if needed, and then click Add.
7. Select the configured connector.
8. Click Start to start the connector.

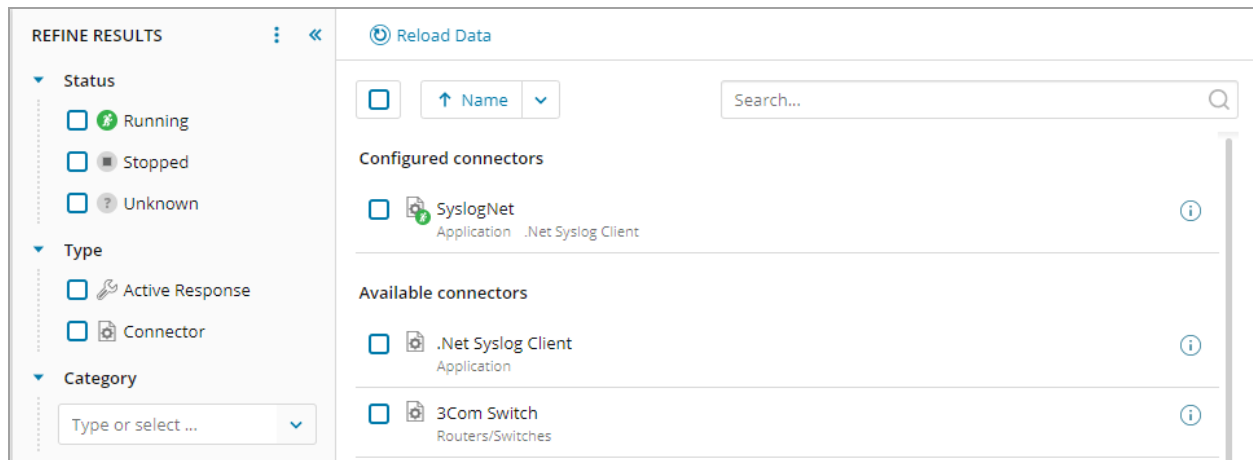
Configure a firewall connector on SEM Manager

After you configure your firewall to log to SEM, configure the corresponding connector on your SolarWinds SEM Manager. Many of the firewall connectors are similar, and some will include unique settings.

The following example describes how to configure a Cisco PIX and IOS connector on your SEM Manager.

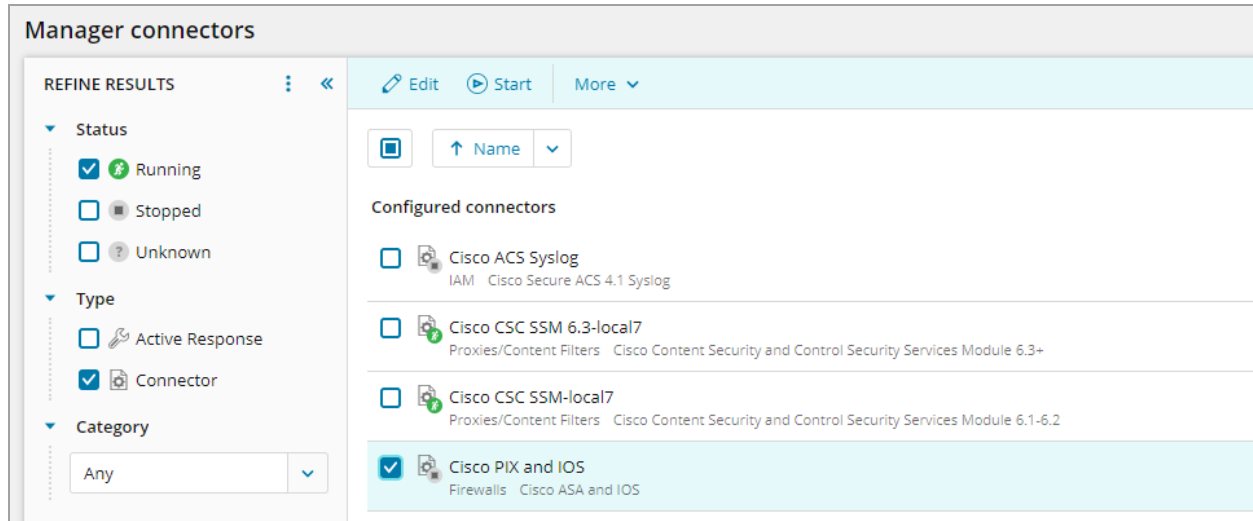
1. Log in to the SEM Console.
2. On the toolbar, click Configure > Manager connectors.
3. Locate the connector to configure.

Type part of the connector name (Cisco PIX) in the search box, or use the filter menus in the Refine Results pane.



4. Select the connector, and then click Add Connector.
5. Complete the connector configuration form. The following fields are common across most connectors:
 - Name: Enter a user-friendly label for your connectors.
 - Log File: Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the SEM appliance (non-Agent devices).
 - Output: Normalized, Raw + Normalized, Raw. You only need to configure these values if SEM is configured to save raw (unnormalized) log messages.
6. Click Add.

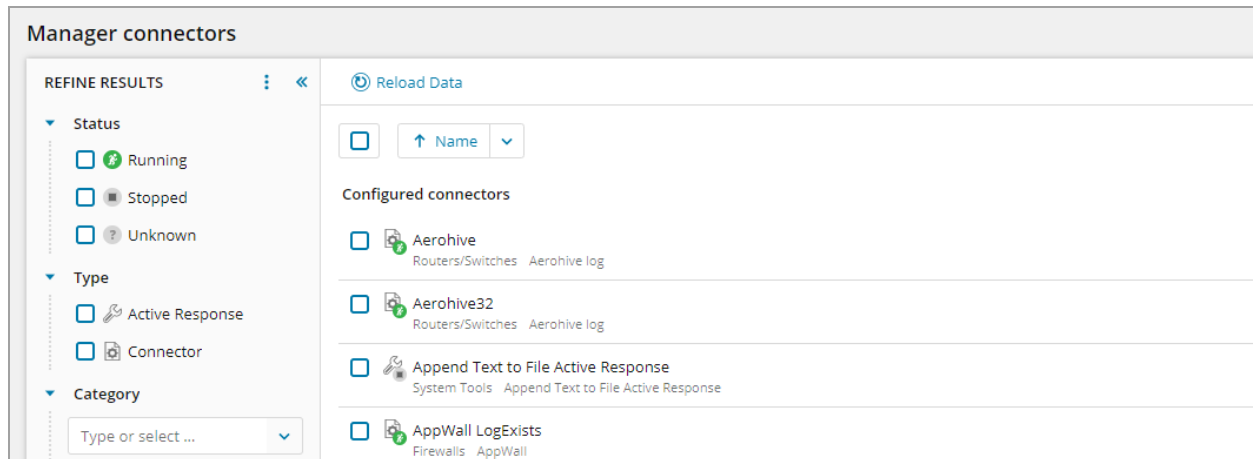
- Under Configured connectors, select your connector, and then click Start.



Verify the alias value associated with the connector

The following procedure applies to devices configured to send logs to SEM. To verify agent connectors, use this same procedure, but apply it to the agent associated with the connector instead.

- Log in to the SEM Console.
- On the toolbar, click Configure > Manager connectors.
- Under Configured connectors, select the connector instance you want to verify.

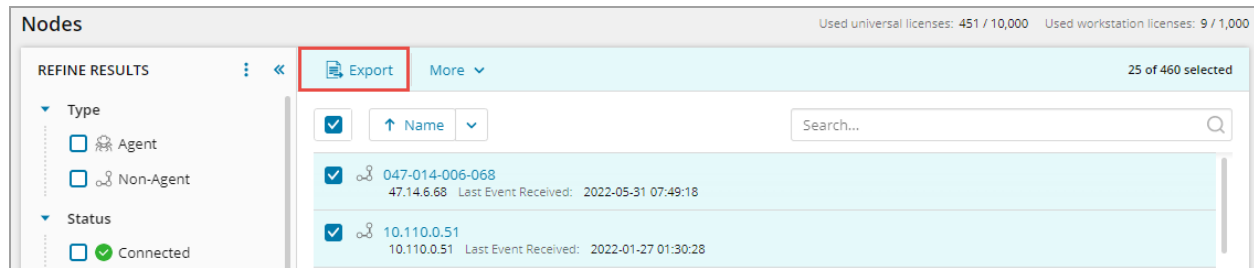


- On the connector toolbar, click Edit.
- Verify the connector name (alias) is correct (change the name, if not), and click Save.
- On the connector toolbar, click Start.

Export the SEM node information

Perform the following steps to export the details of individual or multiple nodes to CSV file.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. If necessary, use the options in the left column to refine the nodes list.
4. Select the node or nodes you want to export.
5. Click Export.



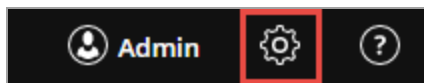
A CSV file containing the details about your selected node(s) is saved to your system.

Manage the SEM system resources

This section describes how to manage the hardware and software resources that SEM requires to work properly.

View the system resources

1. Log in to the SEM Console.
2. On the toolbar, click the Settings icon.



3. In the Settings page, click System Resources.

The System resources window displays with details about the system resources. You can also access the one-click [download debugs](#) feature.

AUTHENTICATION	System resources	
EVENTS LIMITS	Platform	VMware
IMPROVEMENT PROGRAM	CPU reservation	2.00 GHz
LOG FORWARDING	Number of CPUs	2
MANAGE LICENSE	Memory allocation	16.00 GB
	Memory reservation	16.00 GB
SYSTEM RESOURCES	Name	swi-sem
THREAT INTELLIGENCE	Version	2023.4
	IP Address	10.140.205.205
UPDATES		
WEB CONSOLE		
SECURITY		
SHARING		

[Download Debug logs](#)

The following table describes each system resource.

Field	Description
Platform	The Manager platform name, which can be Trigeo SIM, VMware vSphere, or Microsoft Hyper-V.
CPU Reservation	The reserved CPU memory. Reserving CPU memory ensures enough system resources are available for the allocated CPUs.
Number of CPUs	The number of processors allocated to the virtual appliance.
Memory Allocation	The maximum amount of memory the Manager can use. Set this value at or above the reservation value. You can define this value in the VM configuration. Setting memory allocation to a greater value than the memory reservation has little effect on SEM performance.
Memory Reservation	The amount of memory reserved for this system.
Name	The Manager or appliance name.
Version	The Manager or appliance software version.
IP Address	The Manager or appliance IP address.

Allocate CPU and memory resources to the SEM VM

By default, SEM deploys with 8GB of RAM and 2 CPUs on the VMware ESX(i) and Microsoft Hyper-V platforms. For SEM to function properly, allocate sufficient CPU and memory resources to the SEM VM.

SEM collects data from a continuous stream of fluctuating traffic based on user, server, and network activity. The type and volume of traffic varies based on the device sending the traffic and the audit and log settings on those devices.

 See the [SEM system requirements](#) for hardware and software sizing requirements.

 SEM can send SNMP version 3 alerts to Network Performance Monitor (NPM). This configuration allows you to monitor CPU, memory, and other critical SEM components from the SolarWinds Orion Web Console.

About incoming data traffic

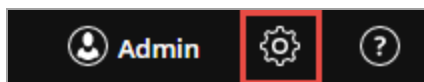
SEM receives data from syslogs and traps using up to 500 connectors that receive data traffic from several supported network devices. These connectors translate (or normalize) the data into a readable and understandable format you can view on the SEM Console.

The events display in the Monitor view, pass through the rules engine for specified actions, and then move into a database for retrieval by the SEM Reports. To process the data in real time, SEM requires system resource reservations from the virtual appliance host.

If your traffic volume exceeds 15 million events per day, reserve additional system resources to support the additional data traffic.

View the system resources

1. Log in to the SEM Console.
2. On the toolbar, click the Settings icon.



3. In the Settings page, click System Resources.

The System resources window displays with details about the system resources. You can also access the one-click [download debugs](#) feature.

AUTHENTICATION	System resources		
EVENTS LIMITS	Platform	VMware	Download Debug logs 
IMPROVEMENT PROGRAM	CPU reservation	2.00 GHz	
LOG FORWARDING	Number of CPUs	2	
MANAGE LICENSE	Memory allocation	16.00 GB	
	Memory reservation	16.00 GB	
SYSTEM RESOURCES	Name	swi-sem	
THREAT INTELLIGENCE	Version	2023.4	
	IP Address	10.140.205.205	
UPDATES			
WEB CONSOLE			
SECURITY			
SHARING			

The following table describes each system resource.

Field	Description
Platform	The Manager platform name, which can be Trigeo SIM, VMware vSphere, or Microsoft Hyper-V.
CPU Reservation	The reserved CPU memory. Reserving CPU memory ensures enough system resources are available for the allocated CPUs.
Number of CPUs	The number of processors allocated to the virtual appliance.
Memory Allocation	The maximum amount of memory the Manager can use. Set this value at or above the reservation value. You can define this value in the VM configuration. Setting memory allocation to a greater value than the memory reservation has little effect on SEM performance.
Memory Reservation	The amount of memory reserved for this system.
Name	The Manager or appliance name.
Version	The Manager or appliance software version.
IP Address	The Manager or appliance IP address.

You can view your reservation settings using vSphere or an SSH client (such as PuTTY). See your VMware vSphere documentation for details about configuring resources, reservations, and storage on a vSphere virtual appliance.

View the vSphere reservation settings for SEM

You can view the reservation settings using the vSphere client. See your VMware vSphere documentation for details about configuring resources, reservations, and storage on a vSphere virtual machine.

1. Log into vSphere and check the **Settings/Reservations** resource.
2. Select SEM from the list (name listed may not be the host name), and view the Summary tab to find the number of CPUs (such as 2 vCPU).



SEM requires at least two CPUs. The highest working setting for any SEM appliance is 16 CPUs.

Provisioned Storage displays the total disk space SEM can use.

If SEM is set for thick provisioning, the used storage is always the total disk space. Thin provisioning allows the used storage to grow to the total amount of storage allocated.

3. On the Resource Allocation tab, record the CPU reservation and the memory reservations values.
4. Check the CPU reservation. The minimum setting is 2.0Ghz. To support a higher processor speed, see your VMware documentation for configuration information.
5. Check the Memory reservation. This value is normally set at 8 GB or higher. This value must be the same value or higher than the reservation.

 Memory reservations can be set as high as 64GB of RAM, which can support over 150 million events per day.

Change the vSphere reservations for SEM

1. Shut down the SEM VM.

See [Start and stop the SEM appliance and agent](#) for details.

2. Right-click the SEM VM to edit the settings.
3. Select the Hardware tab and change the allocated memory size.
4. Select the Resources tab and update the CPU and memory settings.

Set the limit to `unlimited` for both CPU and memory reservations.

5. Click OK to save your changes.
6. Use the vSphere console to start the SEM VM.

View reservations settings using the CMC command-line

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for instructions.

2. At the `cmc>` prompt, type `manager`.
3. Type `viewsysinfo`, and then press Enter.

The system returns memory and CPU information, as well as SEM version and license information.

To return to the `cmc::manager>` prompt, type `:q`.

To exit the manager menu, type `exit`.

To exit the CMC command line, type `exit` at the `cmc>` prompt.

View Hyper-V reservation settings for SEM

Use the following tables to verify your Hyper-V client settings. For details about setting resources, reservations, and storage on a Hyper-V virtual appliance, see your Microsoft Hyper-V documentation.

Memory settings

Setting	Value
Static RAM	8GB, 16GB, 24GB, 32GB, 64GB, 128GB, 256GB
Memory Weight	High

CPU settings (Windows Server 2008 R2)

Setting	Value
Number of processors	2, 4, 6, 8, 10, 12, 14, 16
VM reserve CPU cycles	100%
Limit CPU Cycles	100%
Relative weight for CPU	100%

CPU settings (Windows Server 2012)

Setting	Value
CPU memory details	Click the Advanced tab and set the view and details.
CPU Priority	High
Reserve CPU cycle	100%
Limit CPU cycles	100%

Manage the SEM data storage

By default, the SEM database is allowed 230 GB of the 250 GB allocated to the SEM virtual appliance. This partition consists of three data stores:

- Syslog store
- Events store
- Original or raw log data store (optional)

The **syslog store** consists of all syslog or SNMP log data sent to the SEM VM. SEM reads and processes the data in real time, and then sends it to the event store for long-term storage. SEM stores the original data for 50 days in its original format (in case you need to review it). The data in the syslog store is compressed and rotated daily to maintain a consistent 50-days' worth of data. The amount of data stored here should level off at around the 50-day mark.

The **event store** (the second store) contains all normalized events generated by the SEM Manager and SEM Agents. Data in this store is compressed at ratios of 40:1 to 60:1, which equates to an average compression rate of 95–98%.

The **original log store** (the third store) is an optional store for original or raw log messages. The data in this store can come from SEM agents or other devices logging to the SEM appliance. You can configure if data is sent to this store at the connector level, so not all devices have to store raw log messages in this manner.

Managing your SEM data storage

Depending on your environment requirements, you can use one or more of the following alternate storage methods:

- Back up the SEM VM on a regular basis. This will provide offline storage for your SEM data stores.
- Decrease the number of days that RAW syslog and SNMP data is stored in the Syslog store. This does not include parsed data in the Events store.
- Deploy another SEM VM to be used as a syslog server.
- Deploy another SEM VM to be used as a database server.
- Increase the space allocated to your SEM VM.

For assistance with any of these methods, [submit a ticket to Customer Support](#).

View the SEM database usage numbers

To locate metrics that indicate how the SEM database is used in your deployment, see the following resources:

- Disk Usage summary in the CMC
- Database maintenance report
- Log storage maintenance report

View the Disk usage summary

When you use the command line to log in to SEM, SEM automatically generates a disk usage summary. You can also generate an ad hoc disk usage summary by running the `diskusage` command from the `cmc >appliance` prompt. The two lines to note here are *Logs/Data* and *Logs*.

- The `Logs/Data` figure represents the total space being utilized by the SEM database. This value is presented in the percent % (usedG/allocatedG) format, where *percent* is the percent of the allocated space currently being used, and *allocated* is the total amount of space currently allocated to the SEM database.
- The `Logs` figure represents the amount of space used by the syslog store. This figure is included in the used figure noted above. To figure out how much space is currently being used by the Event store, subtract the `Logs` value from the used value. If you are storing original log messages in the SEM database, the above calculation shows the combined space utilized by both your Event and original log stores.

View the Database maintenance report

To view a snapshot of your current database usage, run the Database Maintenance Report in SEM reports. The report includes the following values:

Value	Description
Disk Usage Summary	Provides disk usage values in terms of the percentage of space allocated to the SEM database.
Disk Usage Details	Provides disk usage values in terms of physical file size.
Database Time Span (days)	Displays how many days worth of live event data is currently stored in the SEM database.
Other Files	Represents the amount of space used by the syslog store.

i For more information, see [Use the SEM Database Maintenance Report to see retention and volume of traffic](#) located in the Customer Success Center.

View the Log storage maintenance report

Run the log storage maintenance report in SEM reports to obtain detailed information about the original log store. If you have not enabled SEM to store original log messages, this report will be blank.

i For more information, see [Live Data Storage Retention in SEM](#) located in the Customer Success Center.

Create a disk usage alert

You can create a disk usage alert from the CMC command line to warn you when a disk partition reaches a preselected use limit. When the limit is reached, an `InternalWarning` event displays in the Monitor view.

You can define the disk use limit by the percentage of unavailable disk space (such as 75 percent), or by the amount of free disk space (such as 58G).

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

2. To access the Appliance menu, at the `cmc>` prompt, enter:

`appliance`

```
////////////////////////////////////
///      SolarWinds Security Event Manager      ///
///              management console              ///
////////////////////////////////////

Detected VMware Virtual Platform
Product Support Key: 
Available commands:
[ appliance ]  Network, System
[ manager ]   Upgrade, Debug
[ service ]   Restrictions, SSH
[ rawlogs ]   Raw logs Configuration/Maintenance
upgrade       Upgrade this Appliance
help          display this help
exit          Exit
cmc >
```

3. To view the disk use of each partition, at the `cmc::appliance>` prompt, enter:

```
diskusage
```

For example:

```
cmc::appliance > diskusage
Checking Disk Usage (this could take a moment)
... ....00.00.00.00.00.00.00.
Partition Disk Usage:
SEM:                35% (991M/3.0G)
OS:                 45% (1.3G/3.0G)
Logs/Data:          1% (901M/234G)
Temp:               2% (252M/5.9G)

Database Queue(s): 4.0K (No alerts queued, 0 alerts waiting in memory)
Rules Queue: 2.1M (0 alerts queued, 0 alerts waiting in memory)
Console Queue: 2.1M (0 alerts queued, 0 alerts waiting in memory)
DataCenter Queue: 2.1M (0 alerts queued, unknown number of alerts waiting
in memory)
EPIC Rules Queue: 2.1M (0 alerts queued, 0 alerts waiting in memory)
Forensic Database Queue: 2.1M (0 data queued, unknown number of data
items waiting in memory)
Logs: 1.3M
Tool Profiles Message Queue: 2.1M (0 alerts queued, unknown number of
alerts waiting in memory)

cmc::appliance >
```

4. At the `cmc::appliance>` prompt, enter:

```
diskusageconfig.
```

Each partition and corresponding disk use limit displays on your screen. For example:

```
cmc::appliance > diskusageconfig
Current Disk Usage Configuration:
# | Partition (filesystem) | Configured limit
=====
1 | SEM (/usr/local)      | 90%
2 | OS (/)                 | 90%
3 | Logs/Data (/var/)     | 10G
```

```
4 |      Temp (/tmp)      |      90%
You can define your disk use limit by the percentage of unavailable disk
space (such as 75%) or the amount of free disk space (such as 58G).
Enter the partition number you want to change (enter 'exit' and press
<Enter> to quit):
```

5. Enter the partition number you want to change, and then press Enter.
6. Enter the disk usage limit value in percentage (such as 75 percent) or size (such as 58G), and then press Enter.

For example, to change the OS disk partition limit in step 3 from 45 percent to 4 percent, enter 40 percent. To change the OS disk partition limit from 1.3 GB to 2.0 GB, enter 2GB.

```
Disk usage limit [90%, sizeK, sizeM, sizeG, sizeT] (default 90%): 40%
Limit '40%' for the 'OS' partition is set.
Press <Enter> to set the next partition. Enter 'exit' and press <Enter>
to quit.
```

7. Press Enter to set the next partition and repeat step 6 (if required).

See [Change the Logs/Data partition](#) for additional information.

8. When you are finished, type `exit`, and then press Enter to quit.

Change the Logs/Data partition setting

When you set the Logs/Data partition (3), a message prompts you to consider changing the database disk configuration using the `dbdiskconfig` command. SolarWinds recommends setting the Logs/Data partition and the database disk configuration to the same value.

Change the database disk configuration

1. Finish configuring your partitions.
2. At the `cmc::appliance>` prompt, enter:

```
dbdiskconfig
```

The following message displays:

```
Current configuration:
DoNotExceedPercentage = 90%

The Manager will restart and apply your changes. To exit, enter 'exit'
```

```
and press Enter.
Enter a new value for DoNotExceedPercentage (default 90):
Please enter an inter number 0-100 or 'exit'
```

3. At the prompt, enter a usage limit value between 0 and 100, and then press Enter.

 If you enter a value less than 25, the partition will be deleted when this value is reached.

The database disk configuration value is saved, and the appliance restarts the Manager Service.

View a disk usage event

In the SEM Console toolbar, click the Live Events tab to view a disk usage event.

For example, if you set the OS disk partition limit as a percentage, the following event displays in the Events viewer table when the limit is reached:

InternalWarning	Manager Monitor Warning! Disk Usage: The OS file system is over 40% full!

If you set the OS disk partition limit as a file size, the following event displays in the All Events grid when the limit is reached:

InternalWarning	Manager Monitor Warning! Disk Usage: The OS files system has under 2G left!

 See [Manage SEM data storage](#) for more information.

SEM tuning and periodic maintenance tasks

Review your [rules](#) on a regular basis. This will ensure that they do not trigger too frequently and SEM uses the processor and memory resources efficiently.

These issues can be caused by:

- Low threshold settings
- Broadly-defined conditions
- Rules that use event groups instead of a single event or subnet of events

The following table provides recommendations for each issue.

Issue	Recommendation
Low threshold settings	Consider increasing the threshold for rules that trigger due to network traffic.
Broadly-defined conditions	Define the rules to apply only to specific user names, IP addresses, or systems. Consider whether a different set of rules with different conditions could serve two distinct areas of your environment.
Rules using event groups instead of a single event or subset of events	Rules that detect authentication or network traffic may trigger on additional events, but may only apply to a subset of those events.

Secure your SEM deployment

This section describes how to secure your SEM deployment to prevent access from unauthorized users.

Review the SEM security checklists

Complete the following tasks to help prevent unauthorized users from accessing SEM.

General security tasks

- ☐ Review the [Security Event Manager Product Forum](#) on THWACK for the latest product information.
- ☐ Configure the subject alternative name (SAN) for the IP address or FQDN/hostname in the SEM Console. The SAN name enables the SEM Manager to detect the SEM agent properly and issue a certificate.

See [Enable the security settings](#) for instructions.

Secure the SEM manager and the SEM consoles

- ☐ Run the activate command from the CMC command line.

This command exports the SSL certificate to provide secure communications between the SEM desktop console and the SEM manager.

See [Run the activate command](#) for instructions.
- ☐ Set the minimum password requirements for the local SEM user accounts.

See [Set the global password policy for SEM users](#) for instructions.
- ☐ Restrict the filters that monitor role users can access.

See [Specify the filters that users assigned the Monitor role can use on the SEM Console](#) for instructions.

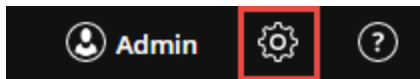
Secure the CMC command-line interface

- ☐ Change the default CMC password.
See [Change the SEM CMC password](#) for instructions.
- ☐ (Optional) Restrict SSH access to the CMC command line interface.
This procedure blacklists all users from logging in to the CMC interface except those users who connect from an explicitly allowed IP address or host name.
See [Restrict SSH access to the SEM CMC interface](#) for instructions.

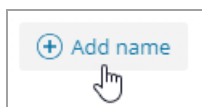
Enable the security settings

Configure the subject alternative name (SAN) for the IP address or FQDN/hostname in the SEM Console. The SAN name enables the SEM Manager to detect the SEM agent properly and issue a certificate.

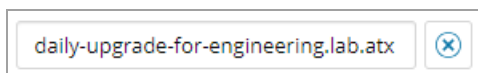
1. Log in to the SEM Console.
2. On the toolbar, click the Settings button.



3. On the Settings page, click the Security tab.
4. In the Agents tab, click Add name.



5. Enter a SAN name in the field. For example:



6. Click Save.

The SAN name is saved to your configuration.

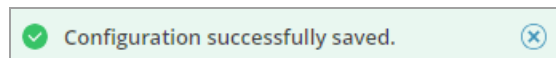
AGENTS

CERTIFICATE

Subject alternative names (SAN)

Add name

A message displays, confirming the update.



Restrict SSH access to the SEM CMC interface

Users who have CMC command-line interface (CLI) access can connect to the SEM VM and perform administrative tasks. You can restrict SSH access to the CMC interface by IP address or host name. This optional procedure blacklists everyone from logging in to the CMC interface except those users who connect from an explicitly allowed IP address or host name.

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

2. Type `service`, and then press Enter.
3. Type `restrictssh`, and then press Enter.
4. Complete the wizard to limit access to the SEM cmc console by IP address or host name. You can enter multiple addresses and host names separated by a space.

Test the restriction by attempting to log in from a blacklisted host or IP address. Repeat the test to confirm that you can log in from whitelisted hosts and IP addresses.

Remove access restrictions from the CMC interface

Perform the following steps to allow users from any IP address or host name to access the CMC interface using SSH.

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

2. Type `service`, and then press Enter.
3. Type `unrestrictssh`, and then press Enter.

4. Complete the wizard to remove access restrictions.
5. Test the restriction by logging in from a previously blacklisted host or IP address.

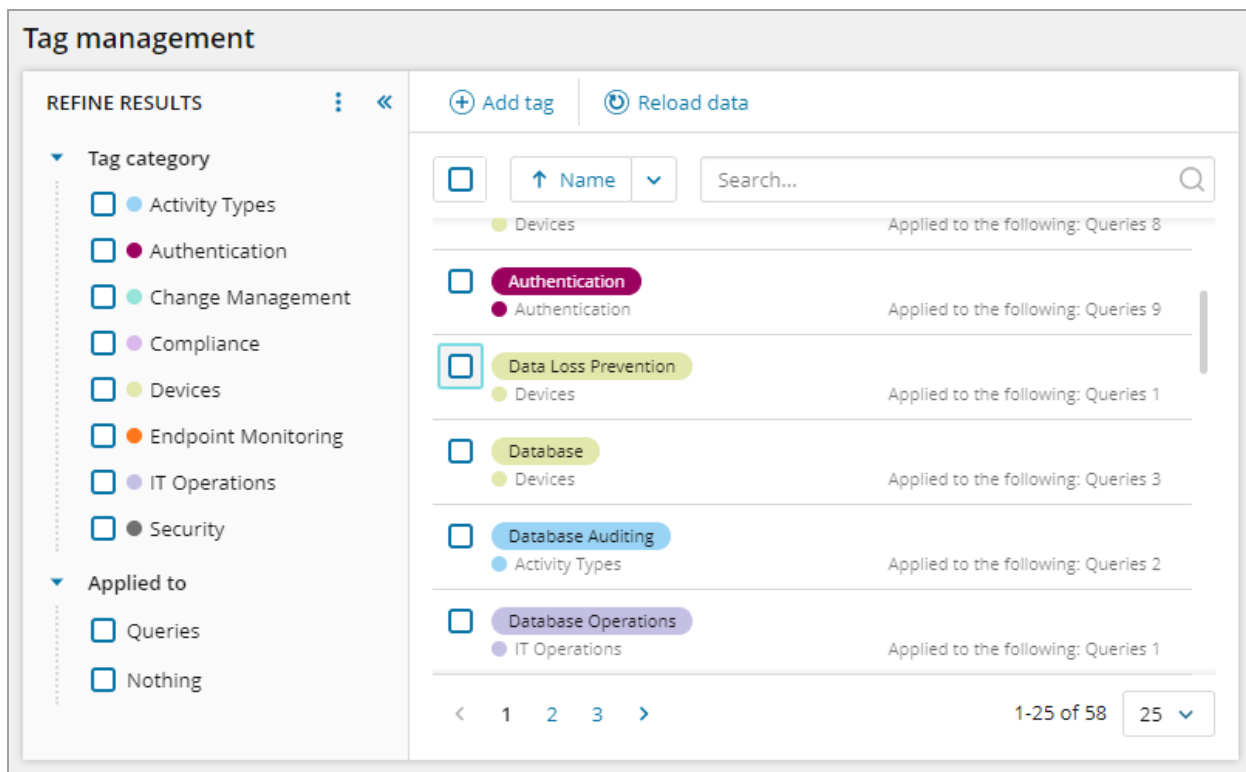
Create and manage tags

Beginning with the 2023.2 release, you can create and view tags from the Tag management window.

Tags allow you to quickly identify specific user activity in your deployment. For example, if you are interested in monitoring a specific event in your deployment, you can [create a new rule](#) with a tag to display the color-coded tag notification on queries matching your defined criteria. You can also apply multiple tags to a single rule or keyword.

SEM includes pre-defined tag categories and tags that you can apply to a rule. You can also create new tags and associate those tags with a tag category. Tags that you create can only be used for saved search queries and cannot be applied to a rule.

To access the Tag management window, log in as an administrator and click Configure > Tag management in the toolbar. Below is an example of the Tag management window.



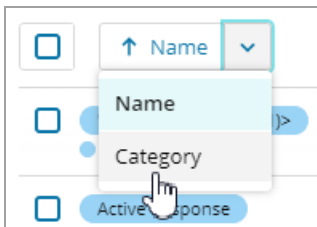
Using the Tag management window, you can:

- [Sort the tag list by category](#)
- [Filter tags by category](#)
- [Filter tags associated with a query](#)

- [Filter tags not associated with a query](#)
- [Search for a tag](#)
- [Add a tag](#)
- [Delete a tag](#)

Sort the tag list by category

Click the Name drop-down menu in the toolbar and select Category.



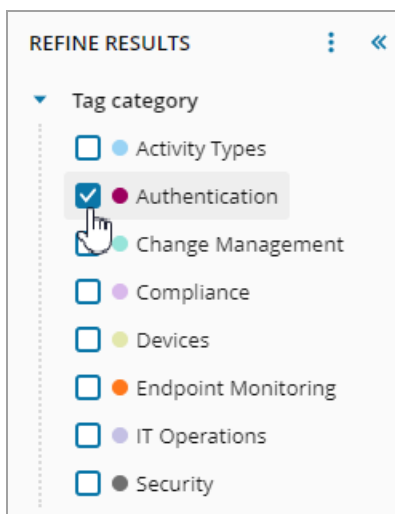
↑ **Category** sorts the list by name in ascending order (A–Z).

↓ **Category** sorts the list by name in descending order (Z–A).

 The default category is Name.

Filter tags by category

In the Refine Results column, maximize the Tag category menu and select a filter. For example, select Authentication.



All tags associated with the Authentication category display in the window.

Tag management

REFINE RESULTS

Tag category

☐ Activity Types
 ☒ Authentication
 ☐ Change Management
 ☐ Compliance
 ☐ Devices
 ☐ Endpoint Monitoring
 ☐ IT Operations
 ☐ Security

Applied to

☐ Queries
 ☐ Nothing

+ Add tag

⌚ Reload data

☐

↑ Name

▼

Search...

☐ Authentication

Authentication

 Applied to the following: Queries 10

☐ General Best Practice

Authentication

 Applied to the following: Queries 0

☐ Local/Domain Authentication

Authentication

 Applied to the following: Queries 0

☐ Remote Device Authentication

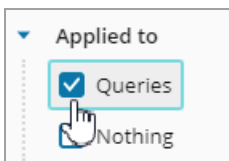
Authentication

 Applied to the following: Queries 0

Click **:** to expand or collapse the Refine Results categories. Click **«** to hide or **»** to display the column.

Filter tags associated with a query

In the Refine Results column, maximize the Applied to menu and select Queries.



All tags applied to a query display in the Tag management window.

Administrator Guide: Security Event Manager

page 193

Tag management

REFINE RESULTS

Tag category

☐ Activity Types
 ☐ Authentication
 ☐ Change Management
 ☐ Compliance
 ☐ Devices
 ☐ Endpoint Monitoring
 ☐ IT Operations
 ☐ Security

Applied to

☒ Queries
 ☐ Nothing

+ Add tag

⌚ Reload data

☐

↑ Name

Search...

☐

<>svg onload=alert(1)>

Activity Types

Applied to the following: Queries 2

☐

Active Response

Activity Types

Applied to the following: Queries 9

☐

Administrative Monitoring

Activity Types

Applied to the following: Queries 5

☐

Anti-Virus

Devices

Applied to the following: Queries 8

☐

Authentication

Authentication

Applied to the following: Queries 10

< 1 2 >

1-25 of 49 25

If you select Queries and a tag category such as Change Management, all Change Management tags applied to a query display in the Tag management window.

Tag management

REFINE RESULTS

Tag category

☐ Activity Types
 ☐ Authentication
 ☒ Change Management
 ☐ Compliance
 ☐ Devices
 ☐ Endpoint Monitoring
 ☐ IT Operations
 ☐ Security

Applied to

☒ Queries
 ☐ Nothing

+ Add tag

⌚ Reload data

☐

↑ Name

Search...

☐

Device Changes

Change Management

Applied to the following: Queries 1

☐

Domain Changes

Change Management

Applied to the following: Queries 3

☐

General Best Practice

Change Management

Applied to the following: Queries 3

☐

Group Changes

Change Management

Applied to the following: Queries 1

☐

Installation/Update

Change Management

Applied to the following: Queries 2

☐

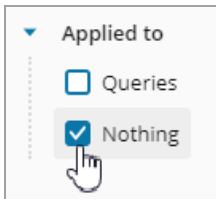
Policy Changes

Administrator Guide: Security Event Manager

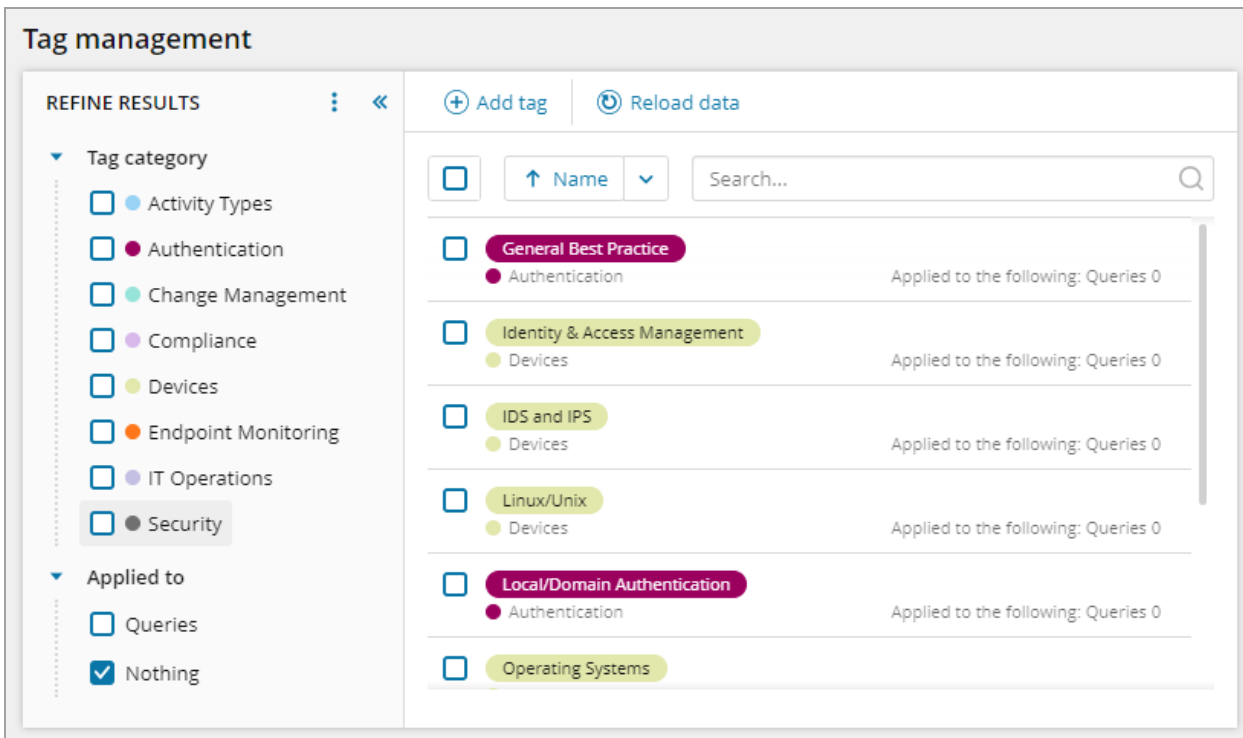
page 194

Filter tags not associated with a query

In the Refine Results column, select Nothing.



All tags not applied to a query display in the Tag management window.



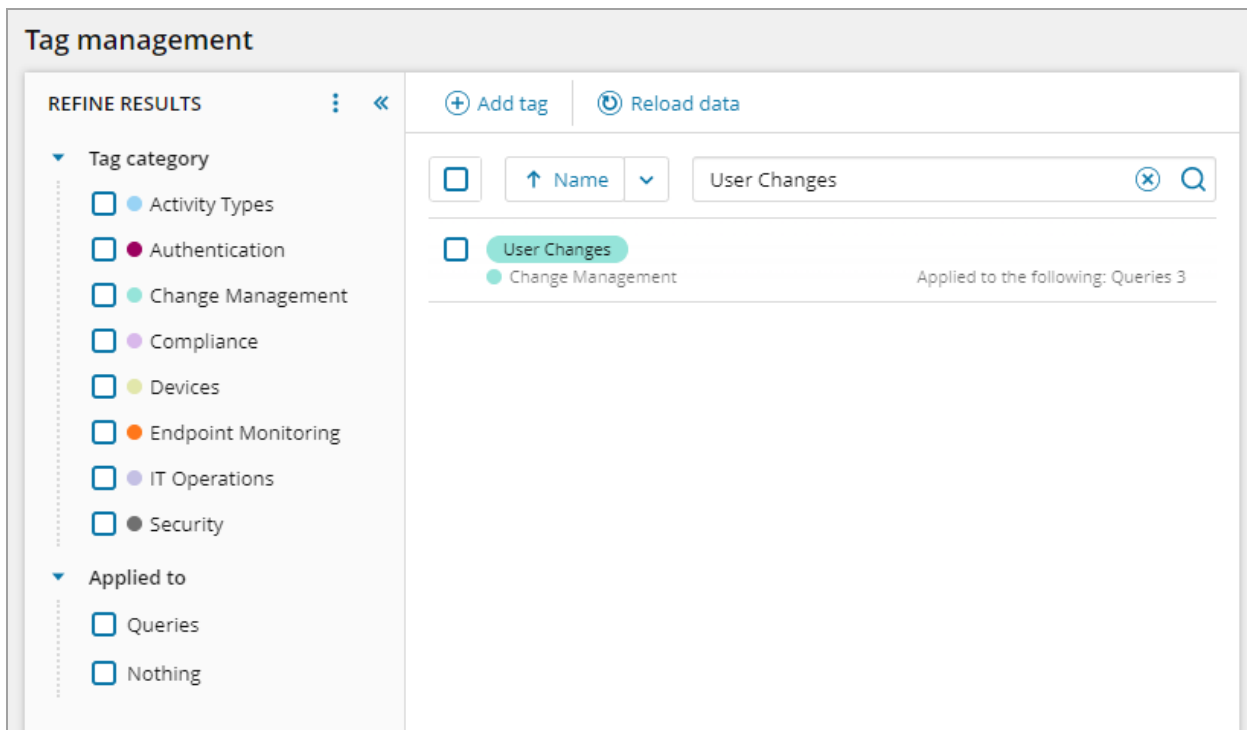
Search for a tag

Enter a tag name in the Search field and then click the magnifying glass  icon or press Enter. For example, search for a tag labeled User Changes.



 Click X in the Search field to clear the search.

The targeted tag displays in the Tag management window with the number of applied queries.



Add a tag

 All categories are color coded and inherit their color from the assigned category.

1. Click Add tag.
2. In the Tag name field, enter a name for your tag. For example:

Tag name

3. Click the Category drop-down menu and select a category for this tag.

Category

● Authentication

4. Click Create.

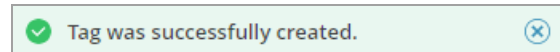
The new tag displays in the Tag management list with a list of queries that include this tag.

☐ **Local and Domain Authentication**

● Authentication

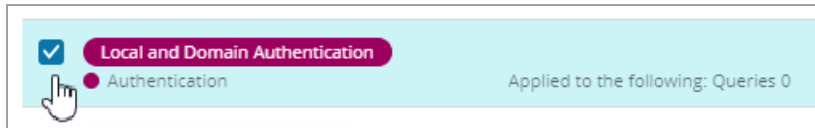
Applied to the following: Queries 0

A confirmation message displays in the Tag management window.



Delete a tag

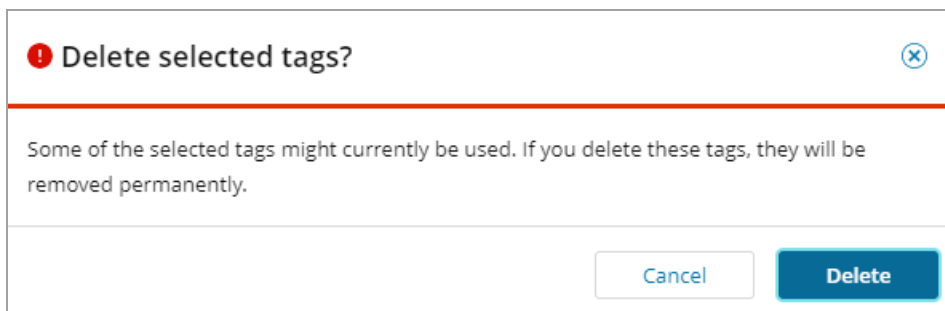
1. Select the tag you want to delete.



2. Click Delete in the toolbar.

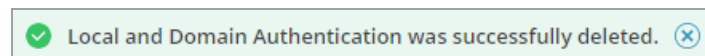


3. Click Delete to continue.



The tag is removed from the Manage tag list and all areas of the SEM Console.

A confirmation message displays in the Tag management window.



Collect and normalize event data using SEM connectors

This section describes how to configure SEM connectors to intercept events sent from a specific product in your network and convert those events into normalized messages that SEM can understand.

 See [SEM connectors](#) for a current list of connectors.

Configure SEM connectors for agent and non-agent devices

You can configure agent connectors for the target products that are installed on or remotely logging to the agent computer. After you configure the agent connectors, SEM can monitor and interact with the products and devices on the targeted computer.

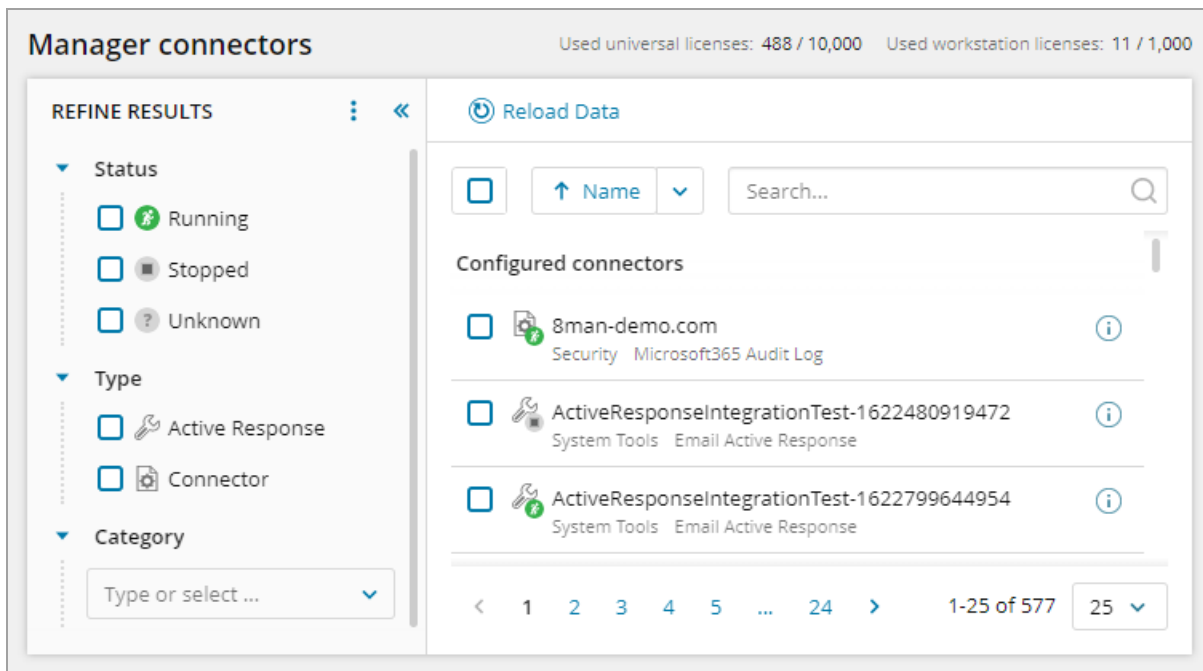
Agent connectors run locally to monitor log files, as well as data logged to the agent computer from remote devices that cannot run an agent. The active response connectors (actors) allow the agent to receive instructions from the Manager and perform active responses locally on the agent computer, such as sending pop-up messages or detaching USB devices.

Use connector profiles to configure multiple agents

Most agents in a network include a few different connector configurations. You can streamline your connector configuration process by [creating connector profiles](#). A connector profile groups agents that share the same connector configuration.

About the Manager connectors screen

The Manager connectors screen displays a list of all connectors that are not configured to a SEM agent. The non-agent connector will be installed on the virtual appliance, and the data will be parsed from this location. You can refine the list by status type, and category.



Configure a connector to monitor non-agent devices

Non-agent devices are devices that cannot host a SEM agent. These devices can include [firewalls](#), [proxy servers](#), [domain controllers](#), and more. You must create a connector to monitor these devices.

1. [Locate a connector](#) for your non-agent device.

 See [SEM connector categories](#) for a list of network security products that can be connected to SEM.

2. Ensure that log data is being recorded for your non-agent source.
3. Log in to the SEM Console.
4. In the toolbar, click Configure > Manager connectors.
5. In the search box, enter the connector name, and then click the magnifying glass icon.
6. Select the checkbox next to the target connector.
7. In the toolbar, click Add Connector.
8. In the Name field, enter a new name, or keep the existing name.
9. Click Add.

The connector displays on the Manager Connectors tab under Configured connector.

10. Under Configured connectors, select this connector.

11. Click Start.

The connector is started and enabled to collect data from the non-agent device.

When SEM recognizes that data is being retrieved from a new IP address that is currently a node, it will be added to the Nodes list automatically for you.

No additional configuration or management is required to monitor non-agent devices. The nodes exist to notify you that data is being received from an IP address.

Apply a SEM connector update package

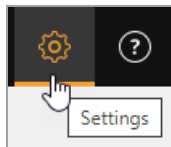
This section describes different options for updating SEM connectors.

On the SEM Console Settings page, you can enable automatic updates for SEM connectors.

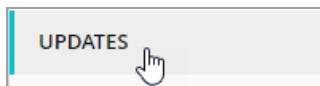
1. Ensure that the following URL is whitelisted from the SEM server in your proxy or firewall:

downloads.solarwinds.com

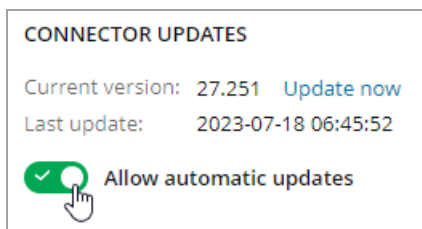
2. On the SEM console toolbar, click Settings.



3. On the Settings page, click the Updates tab in the left column.



4. In the Connector Updates section, click the toggle button to allow automatic updates.



5. Click Save.

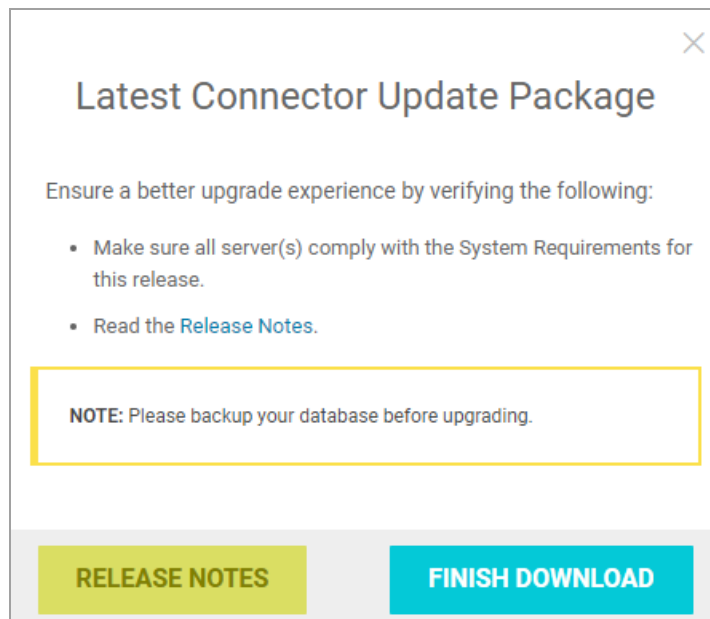
Update SEM connectors manually using the CMC interface

Customer Support occasionally provides stand-alone connector updates to address unmatched data alerts in your environment. These need to be applied manually.

1. Log in to the [SolarWinds Customer Portal](#).
2. Click Downloads > Download Product.
3. Click the Products drop-down menu and select Security Event manager (SEM).
4. Click the Licenses drop-down menu and select your license tier.
5. Scroll down to Upgrade Downloads and locate Latest Connector Update Package.



6. Click Download to download the package.
7. When prompted, read the information in the window, and then click Finish Download.



8. Prepare the update package:
 - a. Extract the update package from the ZIP file, and then open the LEM folder.
 - b. Copy the LEM folder to the root of a network share. For example: C:\share\SEM\.

9. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

10. At the `cmc>` prompt, enter `manager`.

11. At the `cmc::manager>` prompt, enter `sensortoolupgrade`.
12. To start the upgrade process, press Enter.
13. To indicate that the update is located on the network, enter `n`.
14. To continue, press Enter.
15. Enter the path to the network share where the update package is located. Specify the path using the following UNC format: `\\server\volume`
16. To confirm your entry, enter `y`.
17. Enter the domain and user name for a user that can access the share. Use the following format: `domain\user`.
18. To confirm your entry, enter `y`.
19. Enter the password for the user.
Re-enter the password to confirm your entry.
20. To start the update, enter `1`.

The update will take several minutes.

Verify that the configured connectors restart after they are updated by watching for InternalToolOnline alerts in the default SolarWinds Alerts filter on the SEM Console.
21. After the update is finished, type `exit` twice to exit the CMC interface.

Troubleshooting SEM connector upgrades

During the update process, the update script restarts all configured SEM connectors. In most cases, restarted connectors trigger one offline and one online alert in your SEM console.

An `InternalWarning` alert may appear, indicating that a connector started at the beginning of the corresponding log file. This alert may be caused by:

- An unnecessary connector. For example, you could have an NT DNS connector configured on a server that is not running the DNS service.
- A misconfigured connector. For example, you could have a connector pointing to the wrong location for the requisite log file.
- The device associated with the connector rotated its logs while the connector was offline.

Below is the event information for the `InternalWarning` alert.

```
EventInfo: -1:Start location was -1. Init set to 'newest' record,  
record info: 1 - 193 (101 - 293) @ -1. InsertionIP: lab-vm-exc10.lab.exc
```

```
Manager: sem DetectionIP: 10.0.0.1 InsertionTime: 11:51:04 Thu Jun 16 2016
DetectionTime: 11:51:04 Thu Jun 16 2016 Severity: 2 ToolAlias: NT DNS
InferenceRule: ProviderSID: FASTCenter normal error ExtraneousInfo:
Component: FASTCenter:NT DNS Description: -1:Start location was -1. Init set
to 'newest' record, record info: 1 - 193 (101 - 293) @ -1. Detail:
StackTrace:
```

SEM connector categories

The following table describes the various categories of network security products that can be connected to SEM.

The Description column describes how the connectors (sensors and actors) typically work with each type of product or device. The Use with columns indicate if each product type requires Manager connectors, Agent connectors, or both.

 See [SEM connectors](#) for a full list of connectors. If the connector for your product is not listed, [submit a feature request](#).

Category	Description	Use with	
		Managers	Agents
Anti-Virus	This category lets you configure sensors for use with common anti-virus products. These products protect against, isolate, and remove viruses, worms, and Trojan programs from computer systems. To configure an anti-virus connector, the anti-virus software must be currently installed on the Agent computer. Some anti-virus connectors can also be run on the Manager by remotely logging from an Anti-Virus server. Due to software conflicts, SolarWinds recommends running only one brand of anti-virus software per computer.		

Category	Description	Use with	
		Managers	Agents
Application Switch	This category lets you configure sensors for use with application switches. Application-Layer switches transmit and monitor data at the application layer.		
Database	This category lets you configure sensors for use with database auditing products. These products monitor databases for potential database intrusions, changes, and database system events.		
File Transfer and Sharing	This category lets you configure sensors for use with file transfer and file sharing products. These products are used to share files over the local network and the Internet. Monitoring these products provides information about what files are transferred, by whom, and system events.		

Category	Description	Use with	
		Managers	Agents
Firewalls	This category lets you configure sensors and actors for use with applications and devices used to protect and isolate networks from other networks and the Internet. Firewall sensors connect to, read, and retrieve firewall logs. Most firewalls also have an active response connector. These connectors configure actors that interface with routers and firewalls to perform block commands. Actors can perform active responses either via telnet or a serial or console cable. Normally, you will configure these connectors on the Manager. To configure a firewall connector, the firewall product must already be installed on the Agent computer, or it must be remotely logging to an Agent or Manager. Normally, you will configure these connectors on the Manager. You must also configure each firewall's data gathering and active response capabilities separately. For example, configuring a firewall's data gathering capabilities <i>does not</i> configure the firewall's active response settings.		
Identity and Access Management	This category lets you configure sensors for use with identity access, identity management, and other single-sign on connectors. These products provide authentication and single-sign on capabilities, account management, and other user access features. Monitoring these products provides information about authentication and management of accounts.		

Category	Description	Use with	
		Managers	Agents
IDS and IPS	This category lets you configure sensors and actors for use with network-based and host-based intrusion detection systems. These products provide information about potential threats on the network or host, and can be used to raise alarms about possible intrusions, misconfigurations, or network issues. Generally, network-based IDS and IPS connectors are configured to log remotely, while host-based IDS and IPS systems log locally on an Agent system. Some network-based IPS systems provide the capability to perform an active response via their actor connector, allowing you to block an IP address at the IPS device.		
Manager	This category lets you configure sensors for use with the Manager and other Appliances. These connectors monitor for conditions on the Manager that may be informational or display potential problems with the appliances.		
Network Management	This category lets you configure sensors for use with network management connectors. These connectors monitor for different types of network activity from users on the network, such as workstation-level process and application monitoring. Generally, these systems are configured to log remotely from a central monitoring server.		
Network Services	This category lets you configure sensors for use with different network services. These connectors monitor service-level activity for different network services, including DNS and DHCP. Most network services are configured to log locally on an Agent's system. However, some are configured to log remotely.		

Category	Description	Use with	
		Managers	Agents
Operating Systems	This category lets you configure sensors for use with utilities in the Microsoft Windows operating system that monitor system events. This category includes a Windows Active Response connector. This connector configures an actor that enables Windows active response capabilities on Agents using Windows operating systems. This allows SEM to perform operating system-level responses, such as rebooting computers, shutting down computers, disabling networking, and disabling accounts. To configure an operating system connector, the operating system software must already be installed on the Agent computer. If you perform the remote Agent installation, the Windows NT/2000/XP Event Application Logs and System Logs connectors are configured by default.		
Proxy Servers and Content Filters	This category lets you configure sensors for use with different content monitoring connectors. These connectors monitor user network activity for such activities as web surfing, IM/chat, and file downloads, and events related to administering the monitoring systems themselves. Generally, these connectors are configured to log remotely from the monitoring system.		

Category	Description	Use with	
		Managers	Agents
Routers/Switch	This category lets you configure sensors, and in some cases actors, for use with different routers and switches. These connectors monitor activity from routers and switches such as connected/disconnected devices, misconfigurations or system problems/events, detailed access-list information, and other related messages. Some routers/switches have the capability to configure an actor connector to block an IP address at the device. Generally, these connectors are configured to log remotely from the router/switch.		
System Scan Reporters	This category lets you configure sensors for use with different asset scanning connectors, such as vulnerability scanners. These connectors provide information about potential vulnerabilities, exposures, and misconfigurations with different devices on the network. Generally, these connectors create events in the 'Asset' categories in the event tree.		
System Connectors	This category lets you configure the Manager with an external notification system, so SEM can transmit event messages to SEM users via email or pager.		
VPN and Remote Access	This category lets you configure sensors and actors for use with Virtual Private Network (VPN) server products that provide secure remote access to networks. Normally, you will configure these connectors on the Manager.		
Web Server	This category lets you configure sensors for use with Web server products. To configure a web server connector, the web server software must already be installed on the Agent or Manager computer.		

Microsoft SQL Server connector authentication methods

When you create a connector for Microsoft SQL Server, there are two authentication methods currently available:

- SQL Authentication
- Windows Authentication

SQL Authentication

SQL authentication is the simplest solution. When using this authentication method, ensure that:

- A user exists in the database where you are trying to connect.
- Database connectors have the option attribute defined in `DefaultReaderConfiguration`. However, this attribute should be empty for this authentication method.
- The connecting user has Read privileges from the accessed table or view.

Windows Authentication

Windows authentication uses the Windows Users and Active Directory to authenticate to the database. However, the Microsoft Java Database Connectivity (JDBC) driver does not support remote logging as a specific user.

To work around this issue, perform the following steps to configure SEM:

 When you configure the connector, ensure that the Option field includes the following:
`integratedSecurity=true`

1. Verify that:
 - The agent is installed on the machine hosting the targeted database.
 - The agent service is running as User.
 - The connecting user has Read privileges to read from the accessed table or view.
 - The account filled in service has administrator rights for FIM and USB Defender.
2. Log in to the targeted machine as an Administrator.
3. Navigate to Services.
4. In the Services window, right-click the agent service.
5. Select Properties.
6. Select the Log On tab and then select This account.
7. Complete in the credentials for the required user to log in to the database.

8. Click OK.
9. Restart the service.

Monitor firewalls, proxy servers, domain controllers, and more

This section describes how to configure SEM components to monitor and protect specific systems and devices on your network.

Monitor firewalls for unauthorized access

Configure SEM Manager to monitor your firewalls and detect unauthorized access such as port scans, unusual data packets, network attacks, and unusual traffic patterns.

To set up a firewall monitor, configure your firewalls to log to SEM, and then configure a new connector in the SEM Manager. When an unauthorized user attempts to access SEM, the event displays in the default Firewall filter running on the SEM console. You can also create custom filters that display network traffic to and from specific computers, as well as view web traffic and other traffic events across your network.

See [Using the Threat Intelligence feed in SEM](#) on the SolarWinds Success Center for more information.

Configure a firewall to log to SEM

You can configure SEM to collect firewall information from firewalls manufactured by Cisco, Check Point Software Technologies, Juniper Networks, and others. Set your firewall to log to your SEM appliance to centralize its log data with your SEM events.

See the [SolarWinds Success Center](#) or contact [Technical Support](#) for more information.

Configure a firewall connector on the SEM Manager

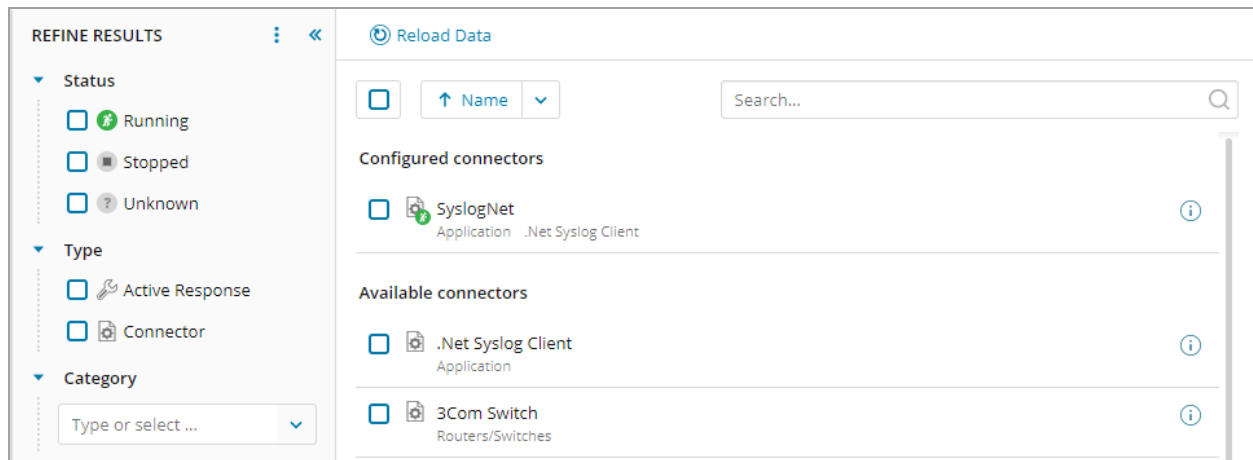
After you configure your firewall to log to SEM, configure the corresponding connector on your SolarWinds SEM Manager. Many of the firewall connectors are similar, and some will include unique settings.

The following example describes how to configure a Cisco PIX and IOS connector on your SEM Manager.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Manager connectors.

3. Locate the connector to configure.

Type part of the connector name (Cisco PIX) in the search box, or use the filter menus in the Refine Results pane.



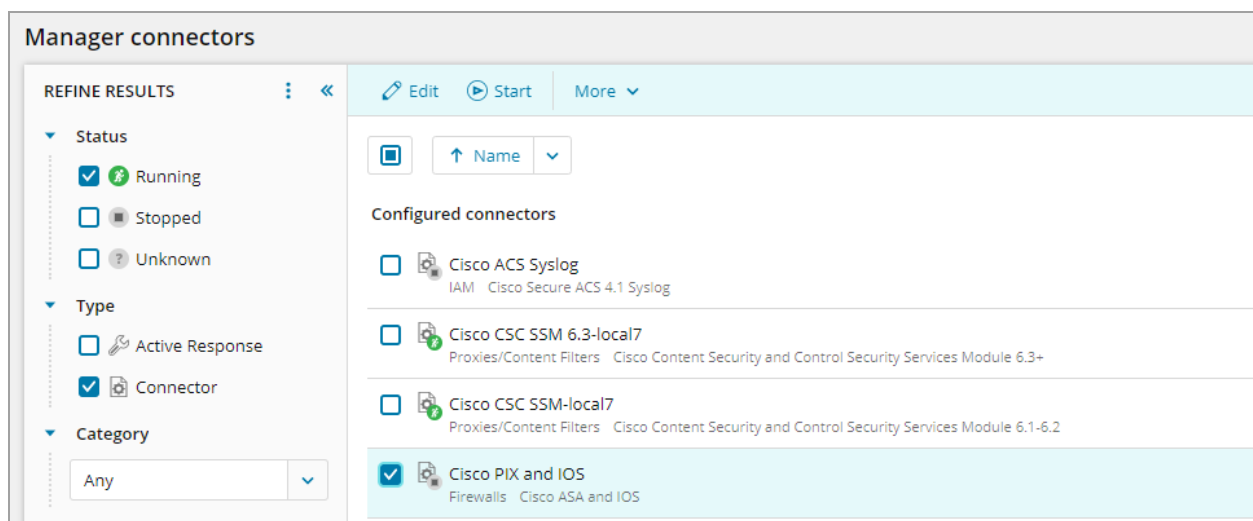
4. Select the connector, and then click Add Connector.

5. Complete the connector configuration form. The following fields are common across most connectors:

- **Name:** Enter a user-friendly label for your connectors.
- **Log File:** Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the SEM appliance (non-Agent devices).
- **Output:** Normalized, Raw + Normalized, Raw. You only need to configure these values if SEM is configured to save raw (unnormalized) log messages.

6. Click Add.

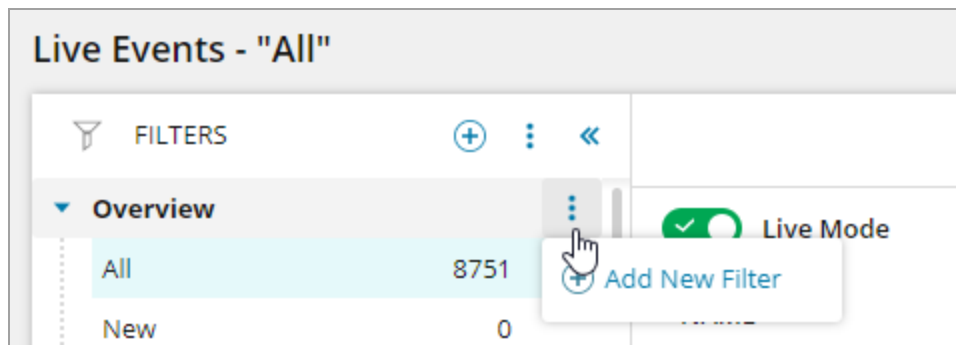
7. Under Configured connectors, select your connector, and then click Start.



View network traffic from specific computers

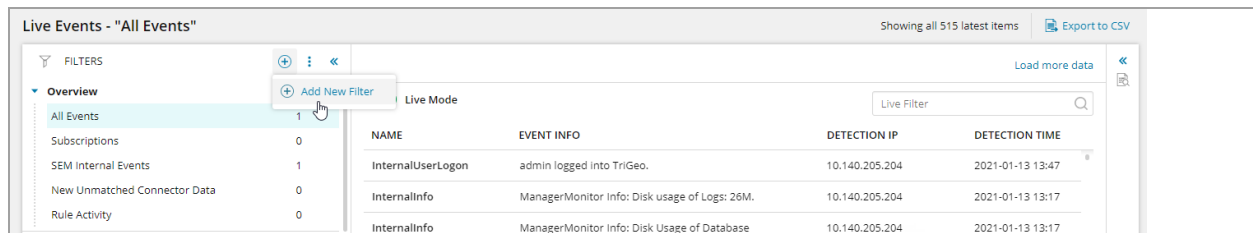
You can create custom filters that highlight specific firewall events. For example, to monitor traffic from a specific computer, create a filter for all network traffic coming from the targeted computer. Use connector profiles and other groups to broaden or refine the scope of custom filters. The following procedure provides an example of creating a filter to monitor all traffic from a targeted computer.

1. On the SEM Console, click the Live Events tab.
2. To create a filter at the group level in the Filters pane, move the mouse pointer over a group heading to expose the vertical ellipsis, and then select Add New Filter.



Or

To create a filter at the root level, click the add  icon, and then select Add New Filter.



The Add new filter window is displayed.

Add new filter

FILTER VALUES

Search...

Events

Event Groups

Use Event groups ups

Directory Service Gr...

Rule Subscription Gr...

Time Groups

Connector Profiles

Constants



Pick an entity to work with
Drag and drop an item from this panel to the query tree.

Name

Network Audit Alerts

Filter is true when

+

Click or drag item from the left panel.

- Enter a descriptive name for your new filter.
- In the panel on the left, expand Event Groups, and then drag Network Audit Alerts into the filter builder.

When you drag a value into the filter builder, the correct drop location is illuminated with a blue line.

- Under Network Audit Alerts, drag SourceMachine into the filter builder.

Add new filter

FILTER VALUES

Search...

Auditable User Ev...

Auth Audit Alerts

Auth Suspicious A...

Change Manage...

File Audit Alerts

EventInfo

ExtraneousInfo

InferenceRule

InsertionIP

InsertionTime

Interface

Name

Network Audit Alerts

Filter is true when

Network Audit Alerts

occurred

AND

Network Audit Alerts.SourceMachine

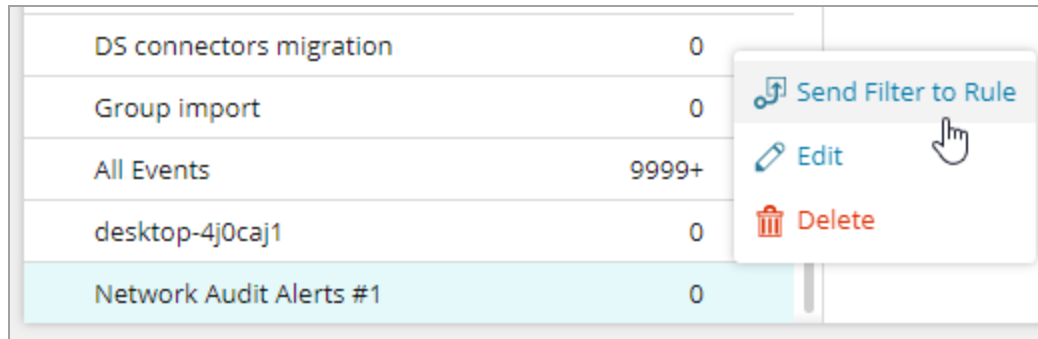
is equal to

Drop item here, or add it

+

Click or drag item from the left panel.

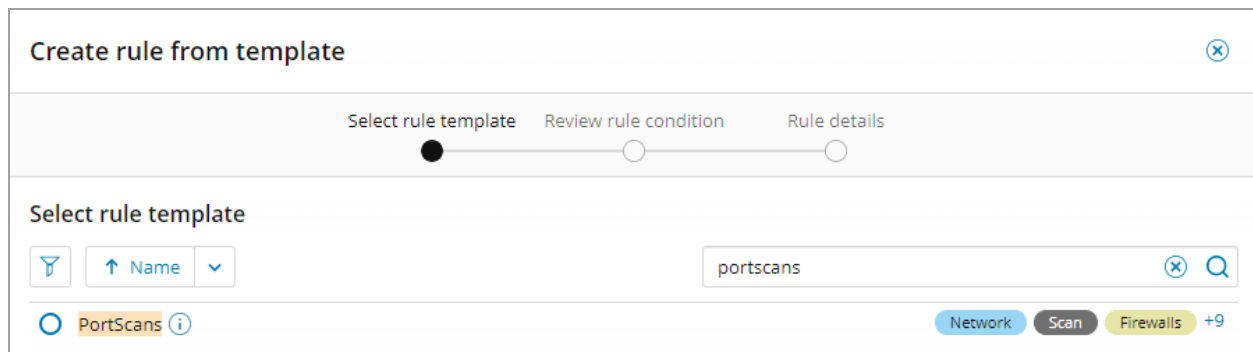
6. Click Drop item here, or add it, enter the domain name of the computer, and click Save.
7. Click Save to return to the Live Events screen.
8. To view associated activity, click the Events tab, and then select your new filter. You can also set up a rule to alert on this activity by moving your mouse pointer over the filter, clicking the vertical ellipsis, and then selecting Send Filter to Rule. Learn more [here](#).



Create and enable a SEM rule to identify port scanning traffic

To identify suspicious firewall traffic indicative of port scanning, clone and enable the PortScans rule. This rule generates a default TCPPortScan event, which the SEM console displays in the default Security Events filter. Use this event to monitor suspicious network traffic and prevent unauthorized access to your firewall.

1. Log in to the SEM Console.
2. In the toolbar, click Rules.
3. On the Rules toolbar, click Create rule from template.
4. In the search box, enter PortScans.



5. Select the PortScans rule template, and then click Next.
6. Review the existing conditions and values. Click Edit and updated if required.

Create rule from template

Select rule template

Review rule condition

Rule details

Review rule condition

⚡ TCPTrafficAudit occurred

And whole rule

occurs at least 10x in 30 sec

in 5 min window

same SourceMachine (TCPTrafficAudit)

distinct DestinationPort (TCPTrafficAudit)

7. Click Next.
8. Review and adjust the rule details where needed.

Rule is true when

⚡ TCPTrafficAudit occurred

+

Click or drag item from the left panel.

And whole rule

occurs at least 10x in 30 sec

in 5 min window

same SourceMachine (TCPTrafficAudit) ✕

distinct DestinationPort (TCPTrafficAudit) ✕

⚙

9. Click Create.

 See [Create a new rule](#) for more information.

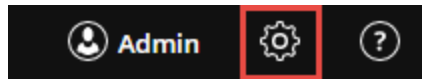
Enable the Threat Intelligence feed

On the SEM Console Settings page, you can enable the Threat Intelligence feed, which enables SEM to detect threats based on lists of known malicious IP addresses. Learn more [here](#).

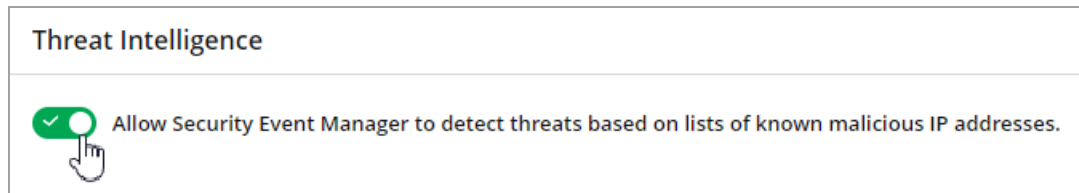
Threat Intelligence is enabled by default. It identifies events as threats by matching event IP information against a list of known bad IP addresses.

 Only administrators have permissions to enable or disable the Threat Intelligence feed. Disabling and re-enabling the Threat Intelligence feed forces a threat intelligence update and creates an `InternalAudit` event. Restarting SEM also forces the Threat Intelligence feed to update.

1. Log in to the SEM Console.
2. On the toolbar, click the Settings icon.



3. Click Threat Intelligence.
4. Drag the toggle to the right to allow SEM to enable the Threat Intelligence feed.



5. Enable the Threat Intelligence feed on the SEM appliance.

See [Using the Threat Intelligence feed in SEM](#) for instructions.

Monitor proxy servers for suspicious URL access

Monitor proxy servers to track network users who attempt to access suspicious websites using partial or complete URL addresses. Configure your proxy server to log in to SEM and set up the appropriate connector on your SolarWinds SEM Manager.

Set your proxy server to log to a virtual appliance

Set your proxy server to log to SEM to centralize its log data with your SEM events. You can integrate proxy servers from popular vendors such as Websense and Barracuda.

Because the integration process is different for each vendor, each proxy server is documented separately in the [SolarWinds Success Center](#). If a knowledge base article is not available, contact [Customer Support](#).

Configure a proxy server connector

After you configure your proxy server to log to your SEM appliance, configure the corresponding connector. Many of the proxy server connectors are similar - with some unique settings.

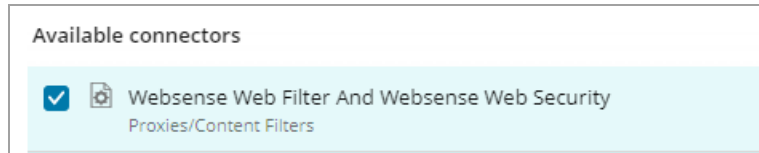
The following example procedure describes how to set up a connector for a Websense proxy server. You can find instructions for additional firewall connectors in the SolarWinds knowledge base.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Manager Connectors.

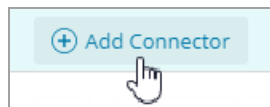
3. In the search box, type Websense Web Filter and then click the magnifying glass icon.



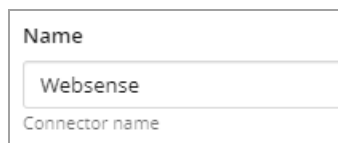
4. Select the Websense Web Filter and Websense Web Security connector.



5. Click Add Connector.



6. In the Name field, enter a new name, or keep the existing name.



7. Click Add.

The connector appears on the Manager Connectors tab under Configured connectors.

8. Under Configured connectors, select this connector.
9. Click Start.

Create and enable the Known Spyware Site traffic rule

You can track when users attempt to access suspicious websites using partial or complete URL addresses by enabling the Known Spyware Site Traffic rule. This rule generates a HostIncident event by default that you can use in conjunction with the Incidents report to notify auditors that you are auditing critical events on your network.

Before you enable this rule, ensure your proxy server transmits complete URL addresses to your SEM Manager by checking the URL field of any WebTrafficAudit event generated by your proxy server. If your proxy server does not log web traffic events with this level of detail, check the events coming from your firewalls, as they can sometimes be used for this rule as well.

1. Log in to the SEM Console.
2. On the toolbar, click Rules.

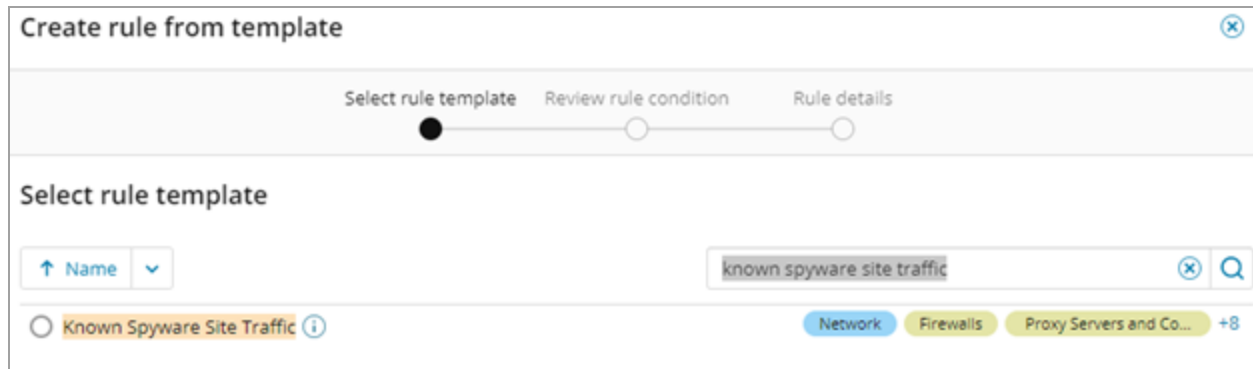
- On the Rules toolbar, click Create rule from template.



- In the search box, enter:

Known Spyware Site traffic

As you type the list of templates is filtered to display your search text.



- Select the Known Spyware Site Traffic rule template, and click Next.
- Review and edit the existing conditions and values where needed, and click Next.
- Review and adjust the rule details where needed, and click Create.

See [Create a new rule](#) for additional guidance.

Monitor antivirus software for viruses that are not cleaned

You can monitor your antivirus software performance by configuring the software to log to SEM. When completed, set up the appropriate connector on the SEM Manager, and then use the SEM console to view events in the default Virus Attack filter.

Configure antivirus software to log to SEM

Set your antivirus software to log to SEM. This process centralizes the antivirus log data with your existing SEM events.

You can integrate SEM with antivirus software from manufacturers such as Symantec and McAfee. See the [SolarWinds Knowledge Base](#) or contact SolarWinds Support for more information.

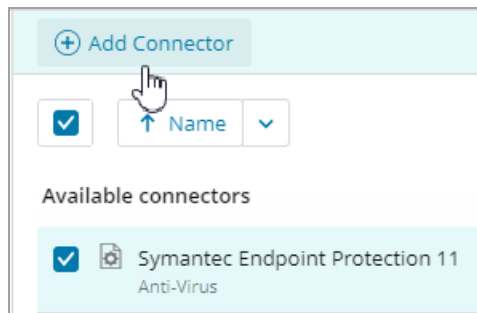
Configure the antivirus connector on the SEM Manager

Perform the following steps to configure the Symantec Endpoint Protection 11 connector on the SEM Manager.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Manager Connectors.
3. In the search box, type Symantec Endpoint Protection and then click the magnifying glass icon.



4. Select the Symantec Endpoint Protection 11 connector, and click Add Connector.



For Symantec Endpoint Protection (SEP), the Log Facility is equal to the local facility on SEM, plus 16. For example, the default Log File for `/var/log/local6.log` on SolarWinds SEM corresponds to Log Facility 22 in your Symantec Endpoint Protection 11 settings.

5. In the Name field, enter a new name, or keep the existing name.

Name

Symantec Endpoint Protection

Connector name

6. Click Add.

The connector appears on the Manager Connectors tab under Configured connectors.

7. Under Configured connectors, select your connector, and then click Start.

Create a SEM rule to track when viruses are not cleaned

Create and enable the Virus Attack – Bad State rule to track virus attacks reported by your anti-virus software. The Bad Virus State User-Defined Group defines a bad state as any virus that is not fully cleaned by your anti-virus software. This includes any virus that is not addressed, quarantined, or renamed.

The default action for this rule generates a HostIncident event, which you can use in conjunction with the Incidents report to notify auditors you are auditing the critical events on your network.

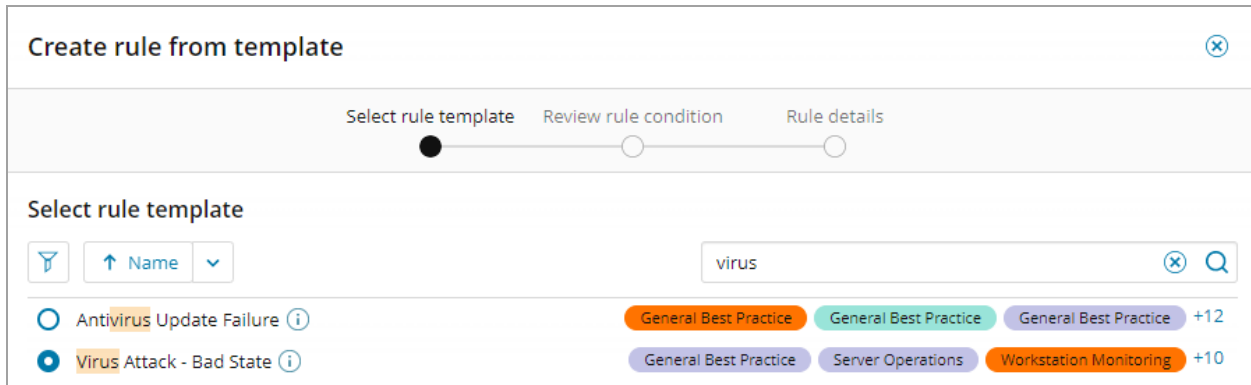
1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. On the Rules toolbar, click Create rule from template.



4. In the search box, enter virus and then click the magnifying glass icon.



5. Select the Virus Attack - Bad State rule template, and then click Next.



6. Review and edit the existing conditions and values where needed, and then click Next.
7. Review and adjust the rule details where needed, and then click Create.

 See [Create a new rule](#) for additional guidance.

Enable Windows file auditing for use with SEM

Enable file auditing in Windows to monitor events related to users accessing, modifying, and deleting sensitive files and folders on your network.

To maximize the value of this type of auditing, enable auditing on a file server where you installed a SEM agent, and only for the specific files and folders you want to monitor. If you enable auditing on all files or folders, the additional auditing may impact SEM performance.

Complete the procedures below to enable object auditing on your server, and then enable file auditing on the files and folders that you want to audit. If Windows is logging the events and your server is running a SEM agent, the SEM console will begin displaying the new file auditing alerts.

 File auditing is only available on systems running Windows Server with Desktop Experience. If you installed Windows Server with Server Core on your system, file auditing is not available.

Enable object auditing in Windows

1. In the Windows Control Panel, navigate to Administrative Tools > Local Security Policy.
2. In the left pane, expand Local Policies, and then click Audit Policy in the left.
3. Select Audit object access in the right pane, and then click Action > Properties.
4. Select Success and Failure, and then click OK.
5. Close the Local Security Policy window.

Enable file auditing on a file or folder in Windows

1. In Windows Explorer, locate the file or folder you want to audit.
2. Right-click the file or folder, and then select Properties.
3. Click the Security tab.
4. Click Advanced.
5. Click the Auditing tab.
6. Click Add. (If using Windows Server 2008, click Edit.)
7. Enter the name of a user or group you want to audit for the selected file or folder, and then click Check Names to validate your entry. For example, enter Everyone.
8. Click OK.
9. Select Success and Failure next to full control to audit everything for the selected file or folder.
10. Optionally, clear Success and Failure for unwanted events such as:
 - Read attributes
 - Read extended attributes
 - Write extended attributes
 - Read permissions

11. Click OK in each window until you are back at Windows Explorer.
12. Repeat these steps for all files or folders you want to audit.

Configure the Windows audit policy for use with SEM

The Windows audit policy determines the verbosity (or the amount of data) that Windows Security logs on domain controllers and other computers in the domain.

See the [Microsoft Technical Documentation website](#) for details about Windows Audit Policy Definitions. These definitions are effective from both a best-practice and compliance standpoint, and are based on customer experience and recommendations from Microsoft.

 See [Audit Policies and Best Practices for SEM](#) in the SolarWinds Success Center for more information.

Requirements

Using the Windows Audit Policy with SEM requires:

- Windows Server 2008 SR or higher
- Permissions to change the Windows Audit Policy at the domain controller and domain level
- SolarWinds SEM installation

Windows Audit Policy

The following events and descriptions are adapted from information available on [the Microsoft Learn website](#). You can query relevant articles on Microsoft Learn by searching for audit policy best practice.

Event	Description
Audit account logon events	Represents user log on or log off instances on a computer logging those events. These events are specifically related to domain logon events and logged in the security log for the related domain controller.
Audit account management	The change management events on a computer. These events include all changes made to users, groups and machines.
Audit logon events	Represents user log on or log off instances from a computer logging those events. These events are logged in the security log of the local computer onto which the user is logging, even when the user is logging onto the domain using their local computer.

Event	Description
Audit object access	Track users accessing objects with their own system access control lists. These objects include files, folders and printers.
Audit policy change	Represents instances where local or group policy changed. These changes include user rights assignments, audit policies and trust policies.
Audit privilege use	Track users accessing objects based on their privilege level. These objects include files, folders and printers, or any object with its own system access control list defined.
Audit process tracking	Logs all instances of process, service, and program starts and stops. This can be useful to track both wanted and unwanted processes, such as AV services and malicious programs.
Audit system events	Includes start up and shut down events on the computer logging them, along with events that affect the system's security. These are operating system events and are only logged locally.

Best practice

The Windows audit policy is defined locally for each computer. SolarWinds recommends using group policy to manage the audit policy at both the domain controller and domain levels.

Set the Windows audit policy

Use the Group Policy Object Editor to set your Windows audit policy settings on desktop systems running at least Windows 8 and servers running at least Windows Server 2008 R2.

 See the [SEM System Requirements](#) for a list of all supported Windows and Windows Server operating systems.

The following procedure applies to setting up sub-category-level auditing.

1. Expand Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Audit > Force Audit Policy Subcategory Settings, and then select enabled.
2. Change or set the policies in Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies.

 When enabling the Force Audit Policy Subcategory option, set the subcategory auditing to enabled and the category-level auditing will be disabled.

Default Domain Controllers Policy

Select Success and Failure for all policies except:

- Audit object access
- Audit privilege use

Default Domain Policy

The Default Domain Policy applies to all computers on your domain except your domain controllers. For this policy, select Success and Failure for:

- Audit account logon events
- Audit account management
- Audit logon events
- Audit policy change
- Audit system events

You can also select Success and Failure for audit process tracking critical processes (such as the AV service) or unauthorized programs (such as games or malicious executable files).

Enabling auditing at the audit level increases the number of events in the system logs. As a result, your SEM database will quickly expand as it collects these logs.

Similarly, there could be bandwidth implications as well. This is dependent upon your network traffic volume and bandwidth capacity. Since Agent traffic is transmitted to the Manager as a real-time trickle of data, bandwidth impact is minimal.

SolarWinds recommends meeting PCI Auditing. However, this may be applicable to other auditing as well.

Category or Subcategory	Setting
System	
Security System Extension	No Auditing
System Integrity	Success and Failure
IPsec Driver	No Auditing
Other System Events	No Auditing
Security State Change	Success and Failure
Logon/Logoff	

Category or Subcategory	Setting
Logon	Success and Failure
Logoff	Success and Failure
Account Lockout	Success and Failure
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	Success and Failure
Other Logon/Logoff Events	Success and Failure
Network Policy Server	No Auditing
Object access	
File System	Success and Failure
Registry	Success and Failure
Kernel Object	No Auditing
SAM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing
File Share	Success and Failure
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	No Auditing
Detailed File Share	No Auditing
Privilege Use	
Sensitive Privilege Use	Failure

Category or Subcategory	Setting
Non-Sensitive Privilege Use	No Auditing
Other Privilege Use Events	No Auditing
Detailed Tracking	
Process Termination	No Auditing
DPAPI Activity	No Auditing
RPC Events	No Auditing
Process Creation	No Auditing
Policy Change	
Audit Policy Change	Success and Failure
Authentication Policy Change	Success and Failure
Authorization Policy Change	Success and Failure
MPSSVC Rule-Level Policy Change	No Auditing
Filtering Platform Policy Change	No Auditing
Other Policy Change Events	Success and Failure
Account Management	
User Account Management	Success and Failure
Computer Account Management	Success and Failure
Security Group Management	Success and Failure
Distribution Group Management	Success and Failure
Application Group Management	Success and Failure
Other Account Management Events	Success and Failure
DS Access	

Category or Subcategory	Setting
Directory Service Changes	No Auditing
Directory Service Replication	No Auditing
Detailed Directory Service Replication	No Auditing
Directory Service Access	Failure
Account Logon	
Kerberos Service Ticket Operations	Success and Failure
Other Account Logon Events	Success and Failure
Kerberos Authentication Service	Success and Failure
Credential Validation	Success and Failure

Configure the USB Defender local policy connector in SEM

The USB Defender Local Policy connector enables a SEM agent to enforce restrictions on USB devices, even when the agent is not connected to the SEM Manager. Instead of using rules when disconnected, the connector uses a list of permitted users or devices. The agent compares the fields in all USB device-attached events to a locally stored white list of users or devices. If none of the fields match an entry on the list, the agent detaches the device.

 See [Configure the Detach USB Device active response in SEM](#) for more information.

When the Agent is connected to the Manager through the network, the Manager rule also applies. Any devices listed in the local white list must be in the User Defined Group for authorized devices. Otherwise, the rule takes effect and the device detaches even though it was allowed by the white list in the USB Defender local policy. When the agent is connected, the USB Defender Local Policy and the SEM rule are active.

1. Create a text file with one entry per line.

This file serves as the local policy. Each entry can be a user name or a USB device ID, from the Extraneous Info field of an attached alert.

2. Log in to the SEM Console.
3. On the toolbar, click Configure > Nodes.

4. Select a node, and then click Manage node connectors.
5. In the search box, type USB defender.
6. Select the USB Defender Local Policy connector, and then click Add Connector.
7. In the Name field, enter a new name, or keep the existing name.
8. Click Browse, and then locate and upload the text file you created above.
9. Click Add.

The connector appears on the Manager Connectors tab under Configured connectors.

10. Under Configured connectors, select your connector, and then click Start.

 The authorized devices in the local white list must also be in the UDG for Manager Detach Unauthorized USB rule or the rule on the Manager enforces detachment when the laptop is connected to the network. In reverse, if you are using a blacklist and the device is in the USB Local Policy and not in the User Defined Group of the rule, the device still detaches.

 Having a device or user in one white list or black list and not in the other is not recommended and yields inconsistent results.

Monitor Microsoft SQL databases for changes to tables and schemas

You can track successful or failed attempts to access your database tables and schemas by installing MSSQL Auditor for Windows on a SEM agent running SQL Server 2008 or later with Profiler. This configuration allows you to monitor your local or remote SQL Server databases.

MSSQL Auditor runs as a service in conjunction with the SEM Agent service.

 You can also [configure the Microsoft SQL audit events connector to process SQL events in SEM](#).

Configure your database servers

Download MSSQL Auditor for Windows from the Customer Portal and install the software on your server. When configured and enabled, the software provides your SolarWinds SEM Agent access to details about any database configuration changes to your database server.

To enable the SolarWinds SEM Agent access to details about your database configuration changes, install the following software on your database server:

- Microsoft SQL Server 2008 or later
- Microsoft .NET 3.5 and 4.0 Framework
- SolarWinds SEM Agent for Windows

When completed, install the MSSQL Auditor for Windows on your server.

Install MSSQL Auditor on a SEM Agent

1. Download the MSSQL Auditor for Windows from the [SolarWinds Customer Portal](#).
2. Double-click the EXE file to start the installation.
3. When prompted, click Next.
4. If you agree with the End User License Agreement, accept the license and then click Next.
5. Click Change to specify an installation folder, or accept the default, and then click Next.
6. Click Install.
7. When the installation is completed, select Launch SolarWinds MSSQL Auditor, and then click Finish.

Configure MSSQL Auditor on your servers

If you did not select Launch SolarWinds MSSQL Auditor after installing the application, you can launch the application from the SolarWinds Security Event Manager program group in your Start menu.

1. Enter the name of the SQL server to monitor in the SQL Server\Instance field, and then click Add Server.

To specify an instance other than the default, enter your server name in the following format:

`Server\Instance`

2. Repeat step 1 for any additional servers you need to monitor.
3. To use an account other than the Local System Account to run MSSQL Auditor on your database server, select This Account in the Run Service As and provide the appropriate credentials.

 SolarWinds recommends using an account in the *sysadmin* role on your database. The account only requires Execute permissions for any stored procedures with the xp_trace prefix.

4. In the Manage Auditor Service section, click Start Auditor Service, and then click OK.

Configure the MSSQL Auditor Connector on a SEM Agent

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. In the Refine Results column, expand Type and select the Agent check box.
4. Select an agent, and then click Manage node connectors.
5. In the search box, type:
MSSQL
6. Select the SolarWinds Security Event Manager MSSQL Auditor connector, and then click Add Connector.
7. In the Name field, enter a new name, or keep the existing name.
8. Click Add.
9. Under Configured connectors, select your connector, and then click Start.
10. Repeat these steps for the MSSQL 2000 Application Log connector.

Monitor Windows domain controllers for brute force hacking attempts

You can monitor your Windows domain controllers using the SEM Agent. After you install and configure the agent, the software tracks brute force and other types of hacking attempts to your domain controllers and reports all events to the SEM Manager.

These events include:

- Unauthorized access to your administrative accounts
- Failed logon attempts
- Account lockouts
- User and group modification
- Change management events

Install the SEM agent on all domain controllers to ensure the SEM Manager captures all your domain events (even if they are not replicated across all domain controllers).

You can view the events on the SEM Console using the change management filter and create custom filters to report all activity on your domain controllers.

Install and configure the SEM agent

When you install the SEM agent, you have the option to install USB Defender. This application works together with the SEM agent to provide real-time notification when a USB drive is installed in your domain controller server. By default, USB Defender generates events related to USB mass storage devices attached to your SEM agents.

For additional security, Microsoft implemented a method in their operating system to log security events. As a result, SEM agents on systems running Windows Server 2008 or Windows 7 require different connectors than the agents running on systems with the legacy Windows operating systems.

If you are running both old and legacy Windows operating systems in your environment, create a connector profile for each operating system.

For SEM agent software and hardware requirements, see the system requirements in the SEM Installation Guide.

Install a SEM agent on a single Windows domain controller

1. Download the SolarWinds SEM Agent installer for Windows from the [SolarWinds Customer Portal](#).

See [Install the SEM agent](#) the SEM Installation and Upgrade Guide for instructions.

2. Extract the ZIP file contents to a local or network directory.
3. Run `Setup.exe`.
4. To start the installation wizard, click Next.
5. Accept the End User License Agreement if you agree, and then click Next.
6. In the Manager Name field, enter the host name of your SEM Manager, and then click Next.

 Do not change the default port values.

7. Confirm the Manager Communication settings, and then click Next.
8. (Optional) To install USB Defender with the SEM agent, select the check box.
9. Confirm the settings on the pre-Installation summary, and then click Install.
10. When the installation is complete, click Next to start the SEM agent service.
11. Inspect the agent log for any errors, and then click Next.
12. To exit the installer, click Done.

The SEM agent is installed on your system and begins sending events to your SEM Manager and SEM Console.

The SEM agent continues running on your system until you uninstall the software or manually stop the SEM agent service.

Configure Windows domain controller connectors

Configure the following connectors that apply to your installation on your Windows domain controllers:

Available connectors

☐	 Windows DHCP Server 2000 Network Services
☐	 Windows DHCP Server 2000/2003/2008 Event Log(Admin) Application
☐	 Windows DHCP Server 2000/2003/2008 Event Log(Operational) Application
☐	 Windows DHCP Server 2000/2003/2008 System Log Network Services
☐	 Windows DHCP Server 2003 And 2008 Network Services
☐	 Windows DNS Server Log Operating Systems
☐	 Windows Directory Service Log Operating Systems

1. On the SEM Console, navigate to Configure > Nodes.
2. Under Refine Results, expand the Type group, and then select the Agent check box.
3. Select an agent, and then click Manage node connectors.
4. Find the connector to configure. Type part of the connector name in the search box, or use the filter menus in the Refine Results pane.
5. Select an available connector, and then click Add Connector.
6. Complete the connector configuration form. The following fields are common across most connectors:
 - Name: Enter a user-friendly label for your connectors.

- **Log File:** Enter the location of the log file that the connector will normalize. This is a location on either the local computer (Agents), or the SEM appliance (non-Agent devices).
- **Output:** Normalized, Raw + Normalized, Raw. You only need to configure these values if SEM is configured to save raw (unnormalized) log messages.

7. Click Add.

8. To start a connector, select a configured connector, and then click Start.

Maintain and monitor multiple domain controller Agents

Connector Profiles help you maintain and monitor multiple domain controllers in your SEM console. You can use these profiles to configure and modify connector settings at the profile level, as well as provide a group you can use to filter incoming event traffic from your SEM Agents to your SEM console.

Create a connector profile based on a single SolarWinds SEM Agent

Follow this procedure to create a connector profile based on a single SEM Agent and a corresponding filter to monitor activity on all systems in the profile.

1. Install the SEM Agent software on all systems you want to include in your new connector profile.

See the [SEM Installation and Upgrade Guide](#) for instructions on how to download and install the SEM Agent.

2. Configure a single SEM Agent to serve as the template for your connector profile.

3. On the SEM menu bar, navigate to Configure > Connector Profile.

4. Click Create Connector Profile.

5. Enter a profile name and description.

6. From the Template list, select the new SEM Agent, and then click Save.

7. In the Groups list, locate your new connector profile.

 Use the Refine Results pane if needed.

8. Next to your connector profile, click , and then select Edit.

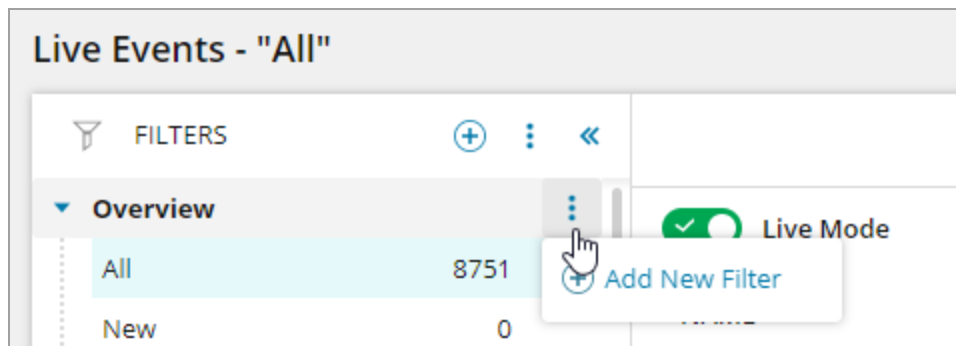
9. In the Available Agents pane, locate the SolarWinds SEM Agents you want to add to your connector profile.

10. Click the arrow next to each SEM Agent you want to add to the Contained Agents pane.

11. When complete, click Save.

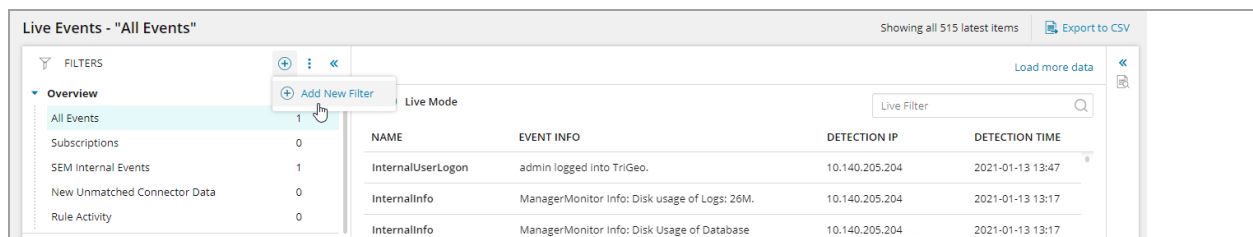
Create a filter for all activity in a Connector Profile

1. Log in to the SEM Console.
2. On the toolbar, click Live Events.
3. To create a filter at a group level in the Filter Values pane, for example, the Overview group, move the mouse pointer over a group heading to expose the vertical ellipsis, and click Add New Filter.



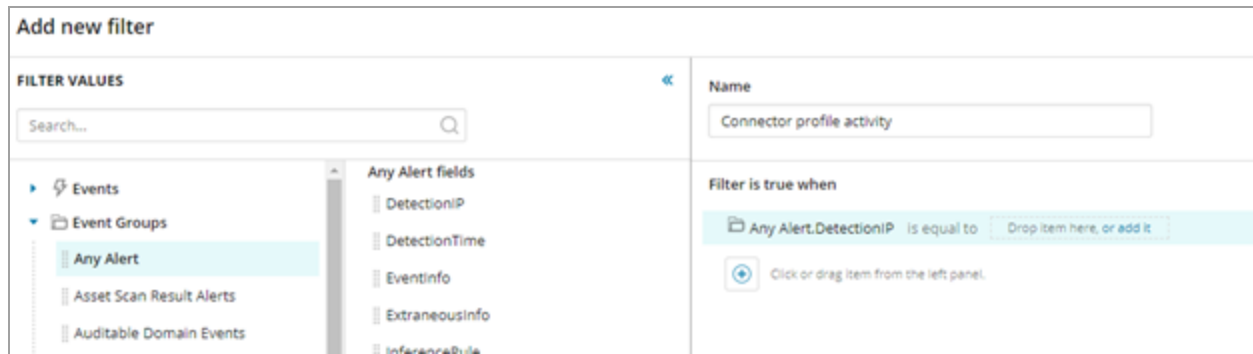
Or:

To create a filter at the root level, click the add  icon, and then select Add New Filter.

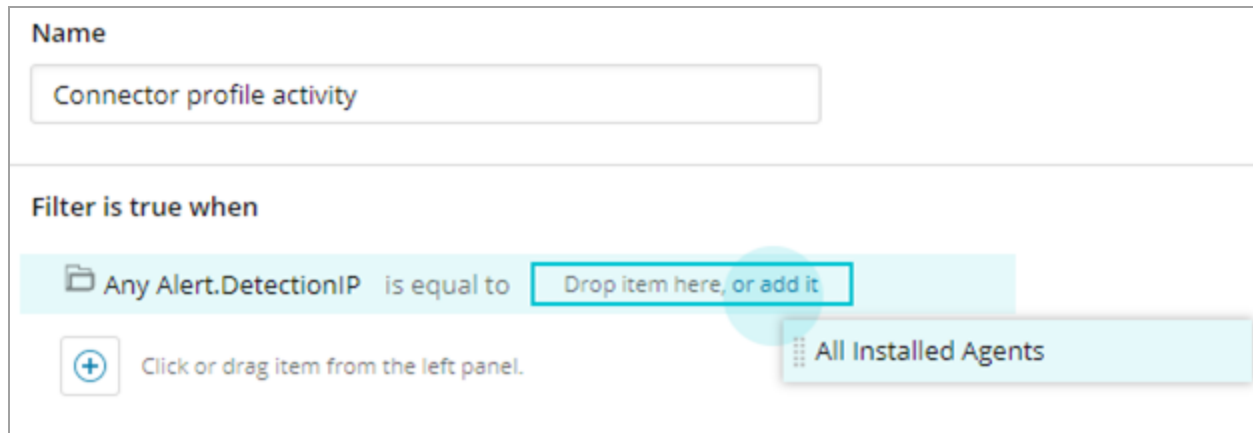


4. Enter a descriptive name for your new filter in the Name field on the right.
5. In the first column under Filter Values on the left, expand Event Groups, and select Any Alert.
6. Drag DetectionIP from the second column on the left into the filter builder.

When you drag a value into the filter builder, the correct drop location is illuminated with a blue line.



7. In the same way, expand the Connector Profiles group, select your profile, and drag it into the filter value drop location.



8. Click Save.

Create and enable a critical logon failures rule

Clone and enable critical account logon failures rule to track failed logon attempts to the default Windows Administrator account. The default action for this rule is to generate a HostIncident event, which you can use in conjunction with the Incidents report to notify auditors you are auditing the critical events on your network.

1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. On the Rules toolbar, click Create rule from template.

Create rule from template

Select rule template

Review rule condition

Rule details

↑ Name

▼

Search...

Agent Offline - Early Shift

Process Auditing

Server Operations

Operating Systems

Agent Offline - Graveyard Shift

Process Auditing

Server Operations

Operating Systems

Agent Offline - Late Shift

Process Auditing

Server Operations

Operating Systems

Agent Offline - Normal Shift

Process Auditing

Server Operations

Operating Systems

Agent Offline - Server

Server Operations

Operating Systems

PCI

+7

Agent Offline Timeout

Server Operations

Operating Systems

General Best Practice

Cancel

Next >

- In the search box, enter:
"critical account" failures
- Select the Critical Account Logon Failures rule template, and then click Next.
- Review and edit the existing conditions and values where needed, and then click Next.
- Review and adjust the rule details where needed, and then click Create.

 See [Create a new rule](#) for additional guidance.

Tune Windows Logging for SEM implementation

After you install and configure your SEM Agents, optimize your SEM deployment by tuning your Windows operating system to log the specific events you want to see in your SEM console and store in your SEM database. Set your group and local policies according to your environment requirements. See [Configure Windows audit policy for use with SEM](#) for more information.

Track Cisco buildup and teardown events

You can enable SEM to track buildup and tear-down events that occur on your network.

To monitor accepted traffic, use the log target in your accepted ACLs instead of the buildup logging. This process lets you control the accepted traffic that will generate an alert. To monitor the information about the actual NAT, consider the event load this will create. Plan a test phase where you turn it on and determine if it is valuable to you for further investigation.

If you need to monitor non-agent log data that was not normalized using a SEM agent, consider the original log message store. This process requires additional disk space.

Also, consider whether you need both buildups and tear-downs, or just buildup messages. The tear-down NAT messages include the same information as the built messages, along with some duration and size information that may or may not be useful. Colleges and universities that use the built messages do not rely on the tear-down messages. They only need to know a connection was established for verification, analysis, and correlation.

Be sure to check your syslog data to determine and enable only those buildup or teardown events are of use.

Tracking Buildup Events

SEM is preconfigured to capture Cisco events 302003, 302009, and 603108. You can configure SEM to capture Cisco firewall buildup events as well.

The primary buildup event to use for TCP tracking is 302013. Other buildup events include 302015, 302017, 302020, 302303, 305009, 305011, and 609011. Check the description of these events in the Cisco System Log Messages Guide located on the Cisco website to ensure you need to capture these events.

Tracking tear-down Events

By default, SEM captures Cisco event 603019. You can also enable SEM to capture Cisco firewall tear-down NAT events.

The teardown sibling to buildup even 302013 is 302014. Other events include 302016, 302018, 302021, 302304, 305010, 305012, 617100, and 609002. You can see description of these events in the Cisco System Log Messages Guide to make sure they are ones you want to capture.

Enabling SEM to track buildup and teardown events

1. Ensure that your firewalls are sending log events to SEM, and that the appropriate SEM connector is monitoring your firewall data.
2. Access the firewalls that contain the buildup and tear-down messages you need to monitor and adjust the severity level of those events from 6 (the default) to 0.

For more information, see the Changing the Severity Level of a Syslog Message section in [Monitoring the Security Appliance](#) (© Cisco 2020, available from [cisco.com](https://www.cisco.com), retrieved on 10/28/2020).

Monitor Windows files, directories, and registry settings using FIM connectors

File Integrity Monitoring (FIM) monitors all Windows file types for unauthorized changes. Using FIM, you can detect changes to critical files to ensure systems have not been compromised.



FIM monitors Windows systems that are configured to process data through the supported SEM agent for Windows. See the [SEM system requirements](#) for more information.

FIM does not support the monitoring of network shares. Only local drives are supported. However, FIM can detect unauthorized modifications to configuration files, executable files, log and audit files, content files, database files, web files, and so on. When FIM detects a change in a monitored file, it logs an event. This event prompts SEM to execute the configured action.

You can build correlation rules to act as a second-level filter to send an alert if certain patterns of activity occur (not just single instances). When an alert is triggered, the data is in context with your network and other system log data.

FIM features

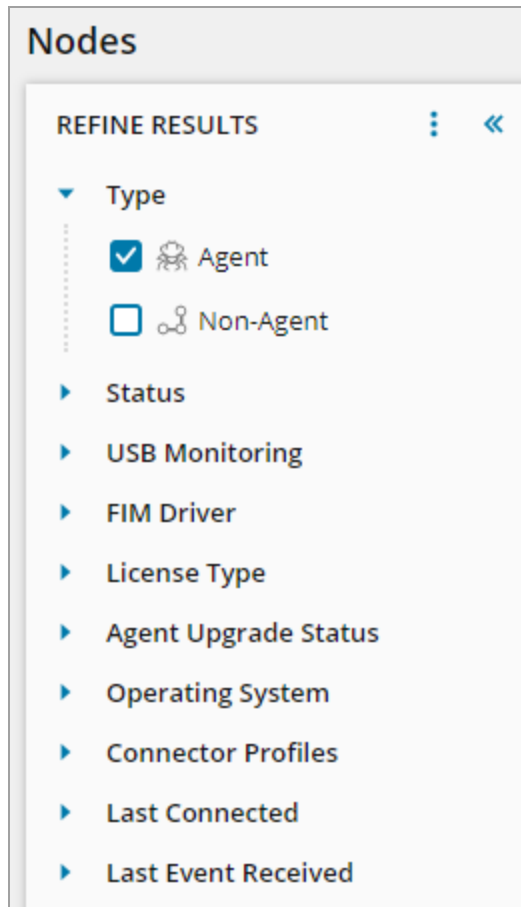
- Monitor real-time access and identify users who change file and registry keys.
- Configure file and directory logic and registry keys and values to monitor different types of access (create, write, delete, change permissions and metadata).
- Standardize configurations across many systems.
- Configure monitoring templates to monitor the basics and create and customize your own monitors.
- Configure templates for rules, filters, and reports to assist in including FIM events.

Start a FIM driver

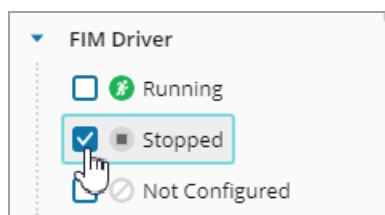
File Integrity Monitoring (FIM) monitors all file types for unauthorized changes. Using FIM, you can detect changes to critical files to ensure systems have not been compromised.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.

3. Under Refine Results, expand the Type group, and select Agent.

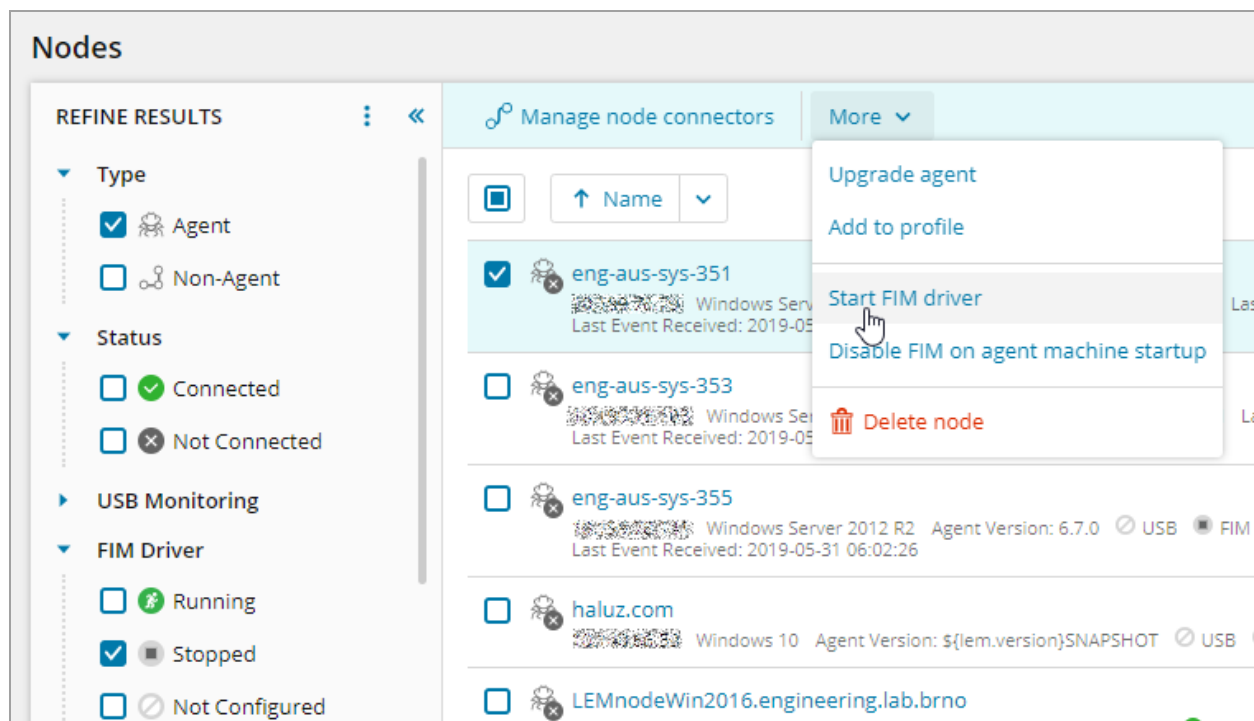


4. Under FIM Driver, select Stopped.

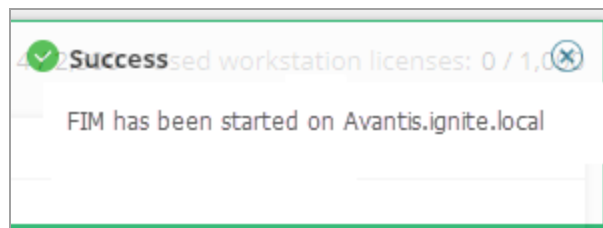


5. Select an agent.
6. On the toolbar, click More > Start FIM Driver.

 If Start FIM driver does not display in the drop-down menu, install a FIM connector on the targeted node. See [Add a FIM connector to a node](#) for instructions.



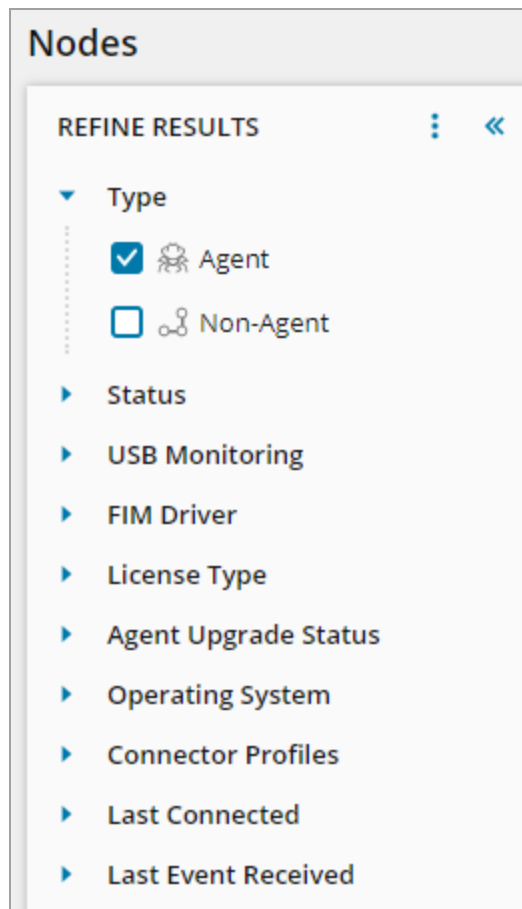
When the configuration is completed, a success dialog displays in the console.



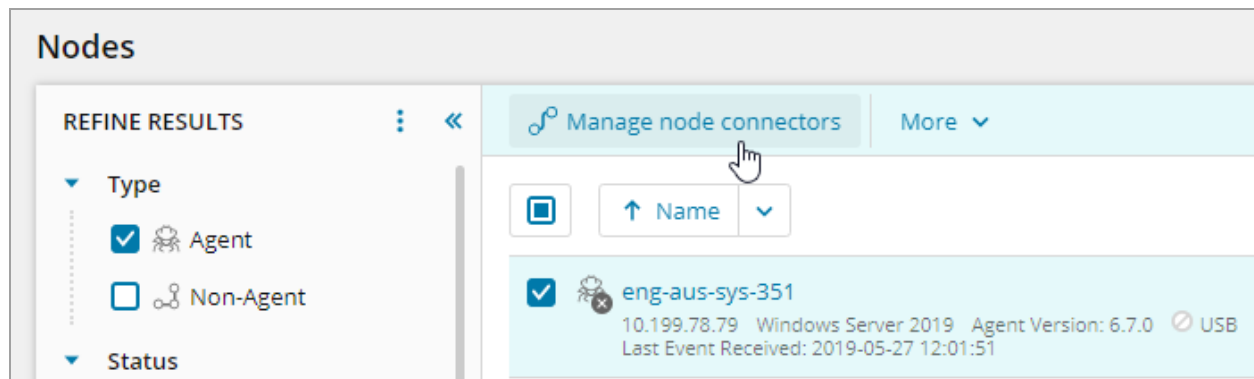
 From the More drop-down list, you can start a FIM driver and enable or disable FIM on agent startup.

Add a FIM connector to a node

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. In the Refine Results pane, expand Type and select Agent.



4. Select an agent and then click Manage node connectors.



5. In the search box, type FIM and then click the magnifying glass icon to view the configured and available FIM connectors.



6. Select a connector, and then click [Create Configuration](#) or [Configure from template](#) on the connector toolbar. Follow the appropriate instructions based on your selection.

7. Click Save.

A confirmation message appears in the upper-right corner of the SEM Console.

8. Under Configured connectors, select your connector.

9. Click Start.

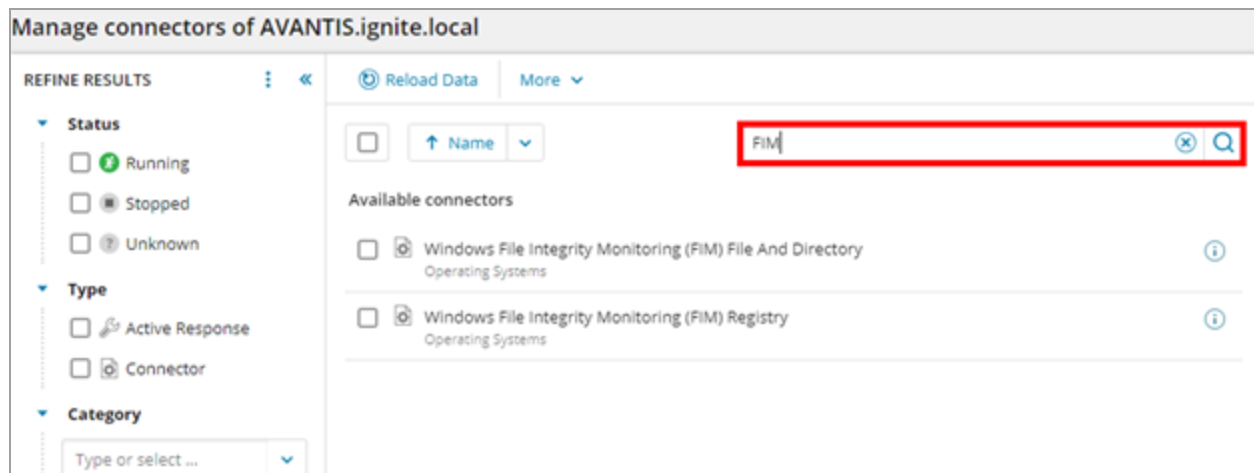
Create a FIM connector configuration

1. Log in to the SEM Console.

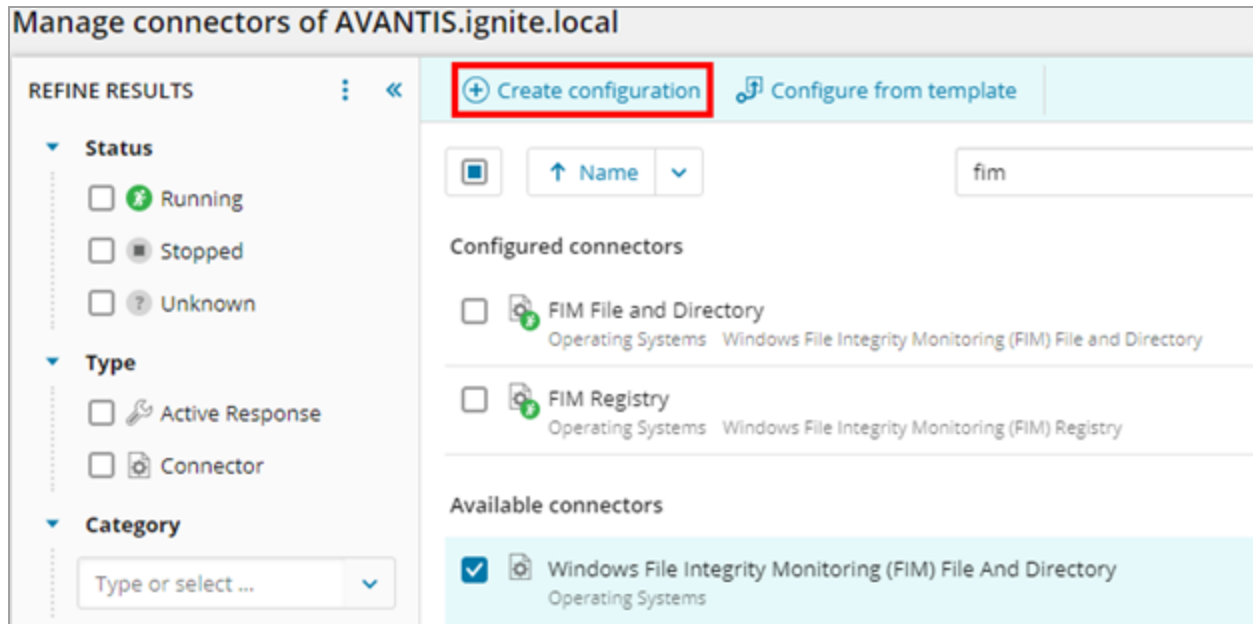
2. On the toolbar, click Configure > Nodes.

3. Select an agent node, and then click Manage node connectors.

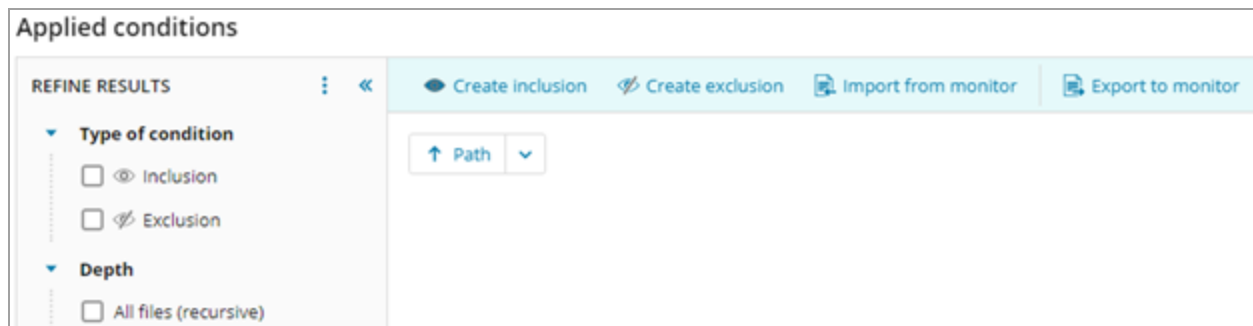
4. In the search box, type FIM and then click the magnifying glass icon. All available FIM connectors display in the window.



5. Select an available connector, and then click Create configuration.



On the Applied Conditions page, you can create inclusions  and exclusions , import conditions from the monitor, and export to monitor.



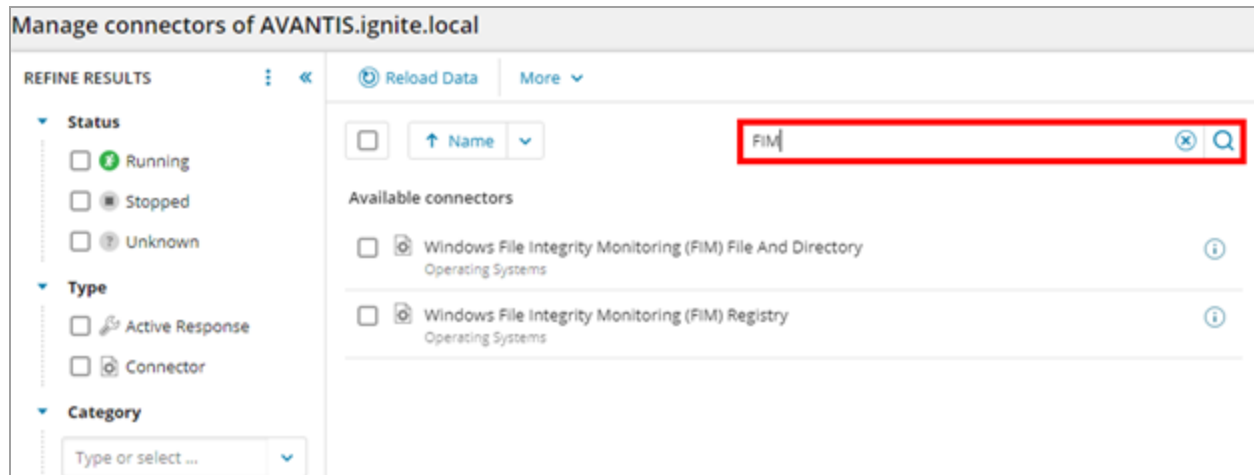
Depending on your connector type, you can [create FIM and directory inclusions](#) and [exclusions](#), as well as [create FIM registry inclusions](#) and [exclusions](#).

6. Establish your applied conditions, and then click Next.
7. Expand and adjust the [FIM advanced configuration settings](#) if necessary
8. Click Create.

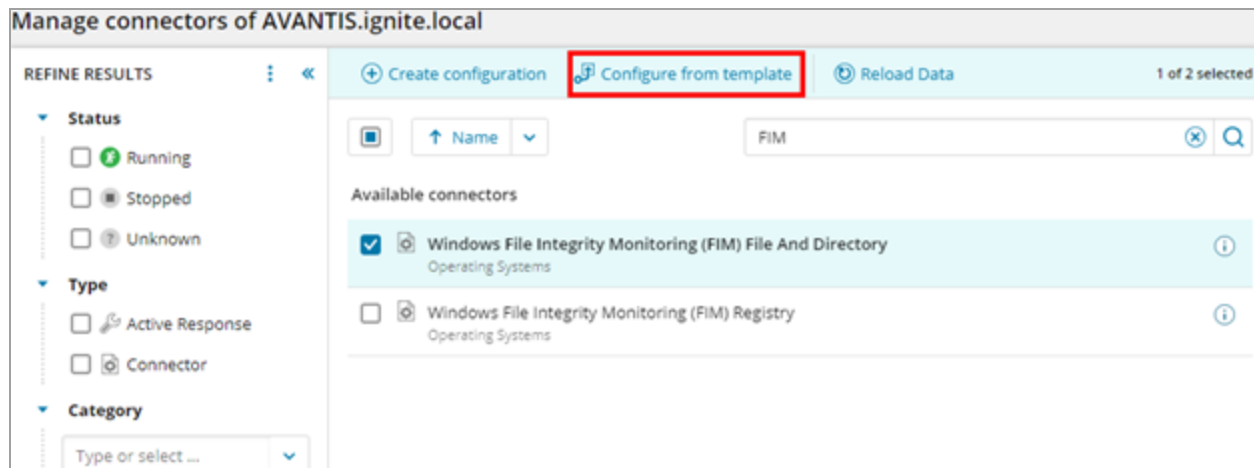
Configure a FIM connector from a template

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. Select an agent node, and then click Manage node connectors.

4. In the search box, type FIM and then click the magnifying glass icon to locate an available FIM connector.



5. Select a connector, and then click Configure from template.



6. In the Name of FIM connector field, keep the current name or enter your own.

Configure from the template

Name of FIM connector

FIM Registry

FIM template

Select a template...

Advanced connector settings

Cancel

Save

7. Click the FIM template drop-down menu and select a pre-defined template.

 Your FIM template results may vary.

Configure from the template

Name of FIM connector

FIM Registry

FIM template

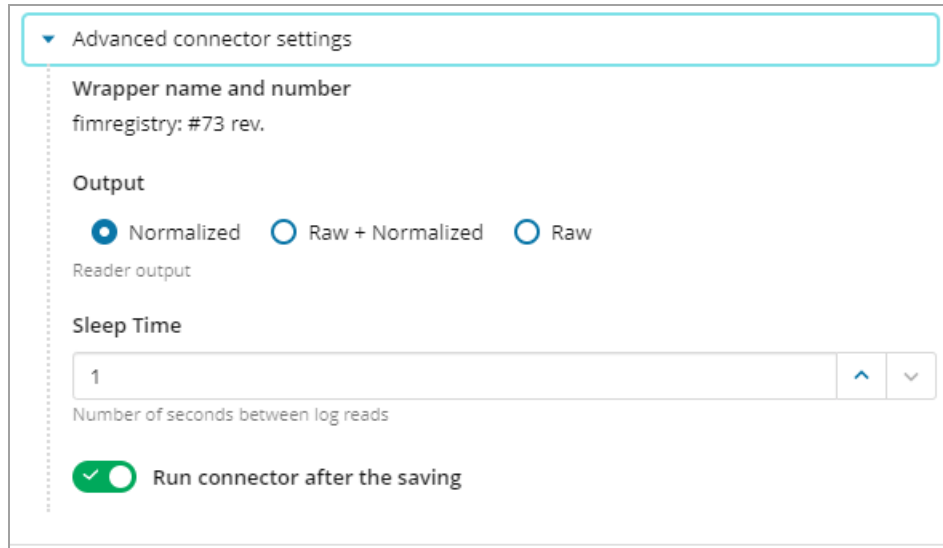
Select a template...

Example - DNS Servers

Example - Proxy Server

Example - Startup Programs

8. Expand the Advanced connector settings.



Advanced connector settings

Wrapper name and number
fimregistry: #73 rev.

Output

☒ Normalized ☐ Raw + Normalized ☐ Raw

Reader output

Sleep Time

1

Number of seconds between log reads

☒ Run connector after the saving

9. Keep the current settings or change the output and sleep time.

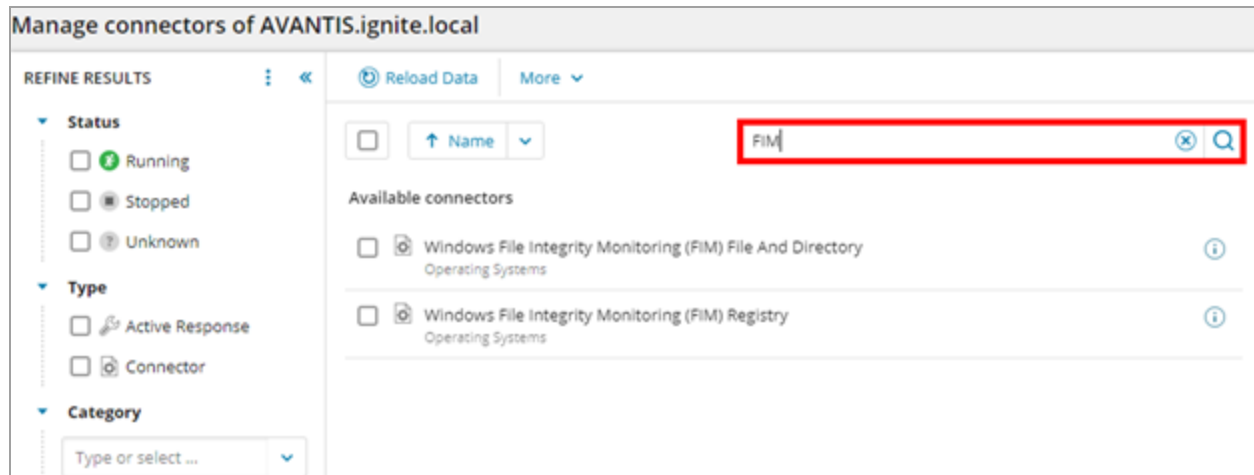
 The sleep time must be a numeric value and cannot be less than one. This is the time (in seconds) the connector sensor is to wait between event monitoring sessions.

10. Drag the toggle to the left if you do not want to run the connector after you save the configuration. Otherwise, go to the next step.
11. Click Save.

Edit a FIM connector configuration

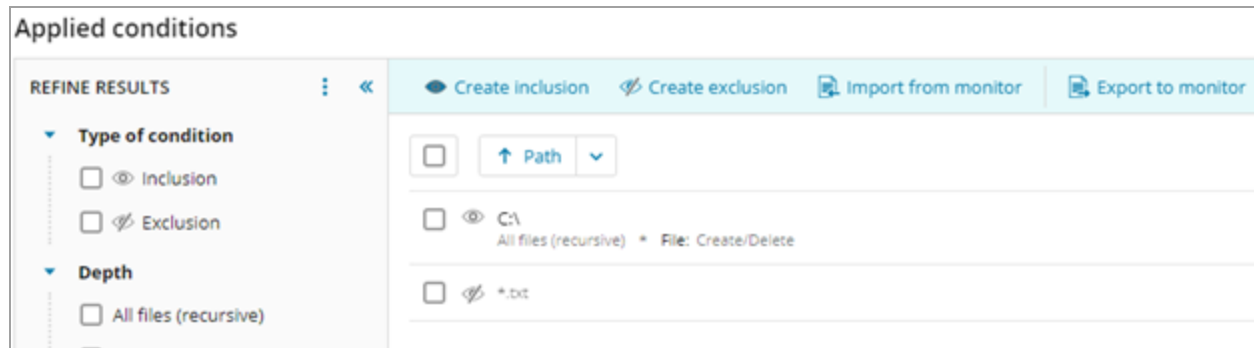
1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. Select an agent node, and then click Manage node connectors.

- To locate an available FIM connector, type FIM in the search box and then click the magnifying glass icon.



- Select a configured connector, and then click Edit.

On the Applied Conditions page, you can create or edit inclusions  and exclusions , import conditions from the monitor, and export to monitor.



Create FIM file and directory inclusions

On the Applied conditions page, you can create, edit, delete, and import inclusions for a FIM file and directory connector.

- Log in to the SEM Console.
- On the toolbar, click Configure > Nodes.
- Select an agent node, and then click Manage node connectors.
- Select a configured FIM file and directory connector, and then click Edit.

5. On Applied conditions page toolbar, click Create inclusions.

Create inclusions

DIRECTORIES TO WATCH

Add path to browse directories

+ Add path

 Browse

Path should be in format: "C:\Users\..."

CONDITION TO WATCH FOR

If this condition is true, an event will be generated. You can set alerts based on these events.

Depth

Contains all keys/values (recursive)

▼

Depth defines which files should be monitored

With mask

Mask should be in format: *.txt

FOR THESE ACTIONS

Directory	☐	Create	☐	Delete
File	☐ Read	☐ Write	☐ Create	☐ Delete
Permissions	☐ Read	☐ Write		
Other	☐ Read	☐ Write		

Cancel

Create

6. Enter one or more paths to the file or directory that FIM is watching and click Add Path.
Click Browse to locate and select one or more files or directories.
7. Select whether the files are recursive or non-recursive.

Recursive	The folder selected and all its sub-folders which match the given mask will be monitored for corresponding selected operations.
Non-recursive	Only the files in the selected folders will be monitored.

8. Enter a mask using the asterisk (*) as a wildcard.

For example:

`*.exe or directory*`

9. For a FIM File and Directory, select Create, Read, Write, and/or Delete for Directory, File, Permissions, and Other operations, and then click Create.

 For information about the Other option, refer to the [Microsoft MSDN information](#).

Create FIM file and directory exclusions

On the Applied conditions page, you can create, edit, delete, and import exclusions for a FIM file and directory connector.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. Select an agent node, and then click Manage node connectors.
4. Select a configured FIM file and directory connector, and then click Edit.

- On the Applied conditions page toolbar, click Create exclusions.

Create exclusion

i This exclusion will only be applied to discs that are monitored with SEM agent version 6.7.0 and newer.

Directories to watch

All locally connected discs

Condition to not watch

Files matching this condition are excluded from File Integrity Monitoring.

Mask

i

Mask should be in format: *.txt

Cancel

Create

- Enter a mask using the asterisk (*) as a wildcard, for example: *.exe or directory*.

 **Directory*** can be used as an exclusion, and it will exclude any file/folder that matches the name from monitoring. It will not exclude the contents of the directory from monitoring.

For example, if there is directory named `DirectoryContent` with files `content1.txt` and `content2.txt` in it, modifications to the directory itself will not be monitored (for example, a permissions change), but changes to the files in that directory will be monitored. You cannot exclude files in specific folders from being monitored, other than set up inclusions to not watch the folder at all.

- Click Create.

Create FIM registry inclusions

On the Applied conditions page, you can create, edit, delete, and import inclusions for a FIM file and directory connector.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. Select an agent node, and then click Manage node connectors.
4. Select a configured FIM registry connector, and then click Edit.
5. On Applied conditions page toolbar, click Create inclusion.

Create inclusions

REGISTRY KEY TO WATCH

Add registry key

+ Add key

 Browse

CONDITION TO WATCH FOR

If this condition is true, an event will be generated. You can set alerts based on these events.

Depth

Contains all keys/values (recursive)

With mask

FOR THESE ACTIONS

Key	☐ Read	☐ Write	☐ Create	☐ Delete
Value	☐ Read	☐ Write	☐ Create	☐ Delete

Cancel

Create

6. Manually enter the registry key to watch, and then click Add Key, or click Browse to locate and select one or more keys.

 You can manually add one or more keys.

7. Select whether the files are recursive or non-recursive.

Recursive	The folder selected and all its sub-folders which match the given mask will be monitored for corresponding selected operations.
Non-recursive	Only the keys in the selected folders will be monitored.

8. Enter a mask using the asterisk (*) as a wildcard, for example: *.exe or directory*.
9. Select Create, Read, Write, and Delete for the Key and Value, and then click Create.

 For information about the Other option, refer to the [Microsoft MSDN information](#).

Create FIM registry exclusions

On the Applied conditions page, you can create, edit, delete, and import exclusions for a FIM file and directory connector.

1. Log in to the SEM Console.,
2. On the toolbar, click Configure > Nodes.
3. Select an agent node, and then click Manage node connectors.
4. Select a configured FIM registry connector, and then click Edit.

- On Applied conditions page toolbar, click Create exclusion.

Create exclusion

i This exclusion will be applied to all registries that are monitored with SEM agent version 6.7.0 and newer which match these keys: HKEY_CLASSES_ROOT, HKEY_LOCAL_MACHINE, HKEY_USERS.

Registry keys to watch

All supported keys

Condition to not watch

Registry values matching this condition are excluded from File Integrity Monitoring.

Mask

Mask should be in format: *.txt

Cancel

Create

- Enter a mask using the asterisk (*) as a wildcard, for example: *.exe or directory*.
- Click Create.

FIM advanced connector settings

Complete the Advanced connector settings form according to the device you are configuring.

The following table lists the fields and descriptions that are common for most connectors.

Field	Description
Wrapper Name and number	An identification key that SEM uses to uniquely identify the properties that apply to this connector. This is read-only information for SolarWinds reference purposes.

Field	Description
Log Data Type to Save	Select either Normalized, Raw + Normalized, or Raw (unnormalized). Storage for original log data must also be enabled on the appliance.
Sleep Time	Type or select the time (in seconds) the connector sensor is to wait between event monitoring sessions. The default (and minimum) value for all connectors is one (1) second. If you experience adverse effects due to too many rapid readings of log entries, increase the Sleep Time for the appropriate connectors. Windows NT-based connectors automatically notify Windows Event Log sensors of new events that enter the log file. Should automatic notification stop for any reason, the Sleep Time dictates the interval the sensor is to use for monitoring new events.
Run connector after saving	When this option is selected, the connector starts when you click Create.

Configure user defined groups

User-defined groups allow you to create groups of values relevant to your IT environment, such as user and computer names, sensitive file locations, trusted IP addresses, and so on. Similar to other groups, user defined groups contain information that can be used in rules and filters.

This section describes how to add and edit values in user-defined groups. You can also create rules that auto-populate user-defined groups with values.

i If Active Directory is available, use *directory service groups* to add user and computer accounts to rules and filters. A user-defined group cannot be synchronized with Active Directory, but a directory service group can synchronize with Active Directory every five minutes. See [Configure Directory Service Groups in SEM](#) for details.

How rules and filters use user-defined groups

Below are a few example rules that depend on user-defined groups:

- A rule that stops SEM from blocking accounts in a user-defined group of trusted administrator accounts.
- A second rule that sends out an alert when an account in the same user-defined group of trusted admin accounts logs in or makes changes.
- A rule that checks a user-defined group containing trusted IP addresses to see if it should block a certain IP address.

Rules and filters typically incorporate user-defined groups in slightly different ways:

- In a rule, user-defined groups are typically used like a white list or black list that tell SEM which events it should include or ignore.
- In a filter, user-defined groups limit the scope of the filter to items that belong to the group.

Rules that use user-defined groups include:

- Authentication - Unknown User
- Critical Account Logon Failures
- Detach Unauthorized USB Devices
- File Audit - Delete Sensitive Files
- Non-Admin Server Logon
- Vendor - Unauthorized Server Logon

Filters that use user-defined groups include:

- Admin Account Authentication
- Domain Controllers (all)

 The Domain Controllers (all) filter uses a connector profile in the constant position by default. You can replace the profile with a user-defined group or a directory service group if the tool profile is not sufficient for your environment. For additional information about connector profiles, see [Create connector profiles to manage and monitor SEM Agents](#).

Create or edit a user-defined group

You can create as many user-defined groups as you need to support your rules and filters.

 You can only add a group to one SEM manager at a time. To copy a group for use with another SEM manager, export the group and then import it into the other manager's Groups grid.

1. Log in to the SEM Console.
2. On the SEM Console, click Configure > User defined groups.
3. On the toolbar, click Create User-defined group.

The Create User-defined group window is displayed.

Create User-defined group

Group elements

Details

+

 Add element

Import elements

No elements added

Add element

Cancel

Next >

4. Click Add element.
5. Complete the fields in the window.

Add new element

Name

Admin

Value

Administrators

Description (optional)

Network administrators

Cancel

Add

- In the Name field, enter a nickname for the element. This name is for reference only.
- In the Value field, enter a value to define the element. You can use wildcard characters, such as asterisks (*), to abbreviate these entries.
- In the description field, enter a description (optional), and then click Add.



In the elements list, you can search for a specific element, and select an element to edit the values or delete it. You can also [export](#) the elements to a CSV file to import into other user-defined groups.

- Continue to add elements as needed, and then click Next.

Create User-defined group

Group elements

Details

+

Add element

Import elements

Export elements

↑

Name

↓

Search...

Q

Admin

Administrators

i

Cancel

Next >

7. Add your group name and description (optional), and then click Create.

Administrator Guide: Security Event Manager

page 260

Create User-defined group

Group elements

Details

Details

Group name

Administrators

Description (optional)

Administrator group

Cancel

Back

Create

The new group is displayed in the user-defined groups list. You can use the group when you configure your rules and filters.

Create User-defined group Reload data	
☐	↑ Name ↓
☐	Administrators Administrator group Modified: 20 Aug 2019, 11:23 AM by admin
☐	Anonymizer Web Sites Web sites used for anonymous browsing. Modified: 01 Jan 2008, 2:00 AM by SolarWinds
☐	Any Alert Every Alert Selected Modified: 25 Mar 2014, 3:13 PM by SolarWinds
☐	Approved DNS Servers Modified: 01 Jan 2008, 2:00 AM by SolarWinds

Edit a user-defined group

1. Select a group in the list.
2. On the toolbar, click Edit.
3. In the Group elements window, you can filter the groups by the modifier and the time last modified.
4. Make any additional changes, and then click Next.
5. Follow the instructions in the window to finish editing the group.

Customize the blank and sample user-defined groups included with SEM

SolarWinds recommends customizing the following blank and sample user-defined groups for your environment:

- Admin accounts
- Admin groups
- Approved DNS servers
- Authorized USB devices
- Authorized VPN users
- Sensitive files
- Service accounts
- Suspicious external machines
- Suspicious local machines
- Trusted IPs
- Trusted server sites
- Vendor and contractor accounts
- Vendor-authorized servers

 The Admin Accounts group is used in several template rules as a placeholder for a custom list of administrative users. This group represents the default administrative accounts in Windows and Unix/Linux environments.

About SEM groups

Groups in SEM are objects used to organize related elements for use with rules and filters. Groups can contain elements such as events, IP addresses, computer names, user accounts, and so on. After a group is defined, it can be referenced from multiple rules and filters.

 Do not confuse groups and roles.

Groups organize related elements into logical units so that they can be used in rules and filters.

Roles restrict the actions that users can perform in SEM. See [About SEM roles](#) for information about SEM role types.

About SEM Group Types

SEM includes the following group types:

- [User-defined groups](#)
- [Event groups](#)
- [Directory Service groups](#)
- [Time-of-day sets](#)
- [Connector profiles](#)
- [Email templates](#)
- [State variables](#)

User-defined groups

User-defined groups contain data specific to your environment, such as user and computer names, the names of sensitive files, trusted IP addresses, and so on. User-defined groups are typically used in rules and filters to whitelist or blacklist events that SEM should include or ignore when evaluating rules and filters.

SEM ships with more than two dozen user-defined groups that need to be populated with values for your environment. See [Configure user-defined groups](#) for more information. You can also create rules that auto-populate user-defined groups with values.

Event groups

Event groups gather similar events into a single category for use with rules and filters. For example, create an event group for events that should all trigger the same response from SEM. If an event in the group occurs, SEM will fire the rule for that group.

SEM ships with more than a dozen predefined event groups, such as: virus/scanner events, process start/stop events, change management events, and so on.

Directory Service groups

Directory Service groups (DS groups) are groups of users or computers that SEM imports from Microsoft Active Directory. DS groups are synchronized with Active Directory every five minutes. Use DS Groups in rules and filters to match specific users or computers. For example, use a DS group in a filter to limit the scope of events to only users or computers in that group.

Time-of-day sets

Time-of-day sets are defined time periods that you can use in rules and filters. Use time-of-day sets to perform specific actions at different hours of the day. For example, if you define a time-of-day set for Working Hours, and another for Outside Working Hours, you can assign different rules to each set.

SEM ships with the following predefined time-of-day sets: business hours, early shift, graveyard shift, late shift, normal shift, and reboot cycle.

Connector profiles

Connector profiles are groups of Agents with common connector configurations. Most Agents in a network only have a few different network security connector configurations. Using connector profiles, you can group Agents by their common connector configurations, and enable your rules and filters to include or exclude the Agents associated with a profile.

Email templates

Email templates are pre-formatted email messages that your rules use to notify you when an event occurs.

State variables

State variables are used in rules to represent temporary or transitional states. For example, you can create a state variable to track the state of a system, setting it to a different value depending on whether the system comes online or goes offline.

How groups are added to filters and rules on the SEM Console

This section describes how groups are used in filters and rules.

Use groups in filters

You can access the filter builder by selecting Live Events from the top menu, clicking the  icon in the left panel, and then clicking Add new filter.

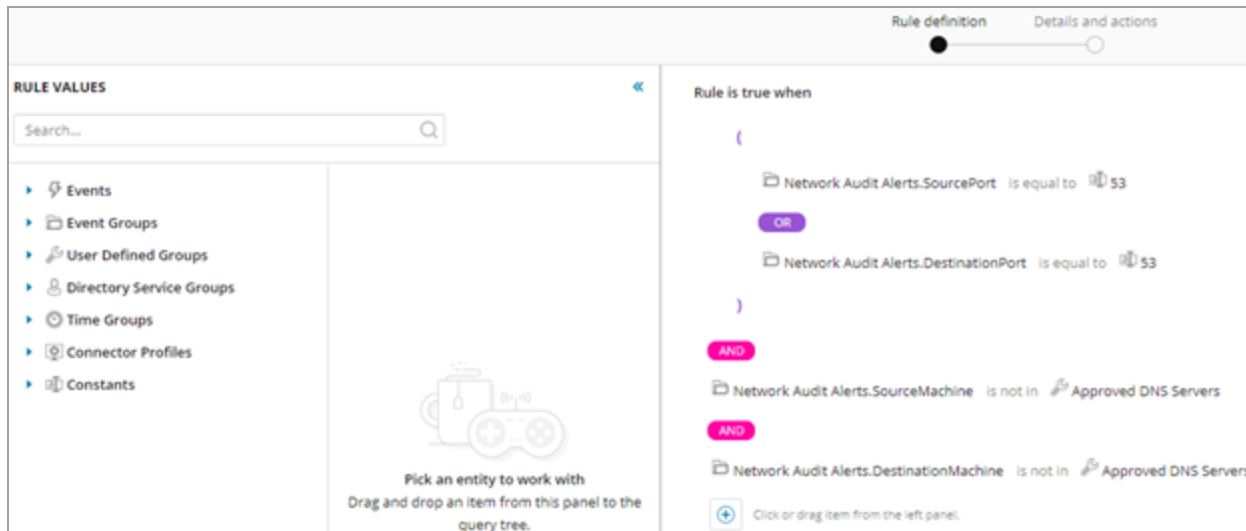
In the left panel, groups are organized by group type. In the right panel, the filter builder shows that the Service Audit Alerts event group is included as a condition of the filter.

Add new filter

FILTER VALUES		Name
Search...		Service Alerts
- Events - Event Groups - User Defined Groups - Directory Service Groups - Rule Subscription Groups - Time Groups - Connector Profiles - Constants	Filter is true when  Service Audit Alerts occurred  Click or drag item from the left panel.	

Use groups in rules

You can access rule definitions by selecting Rules > Create New Rules. Groups are organized by group-type in the left panel.



In the right panel, the rule definition builder shows two different groups in the rule conditions:

- Network Audit Alerts event group,
- Approved DNS Servers user-defined group

Four child fields are specified in the Network Audit Alerts event group:

- SourcePort
- DestinationPort
- SourceMachine
- DestinationMachine

Import user-defined group elements

If you have group elements saved to a Comma Separated Values (CSV) file, you can import those elements into your user-defined group.

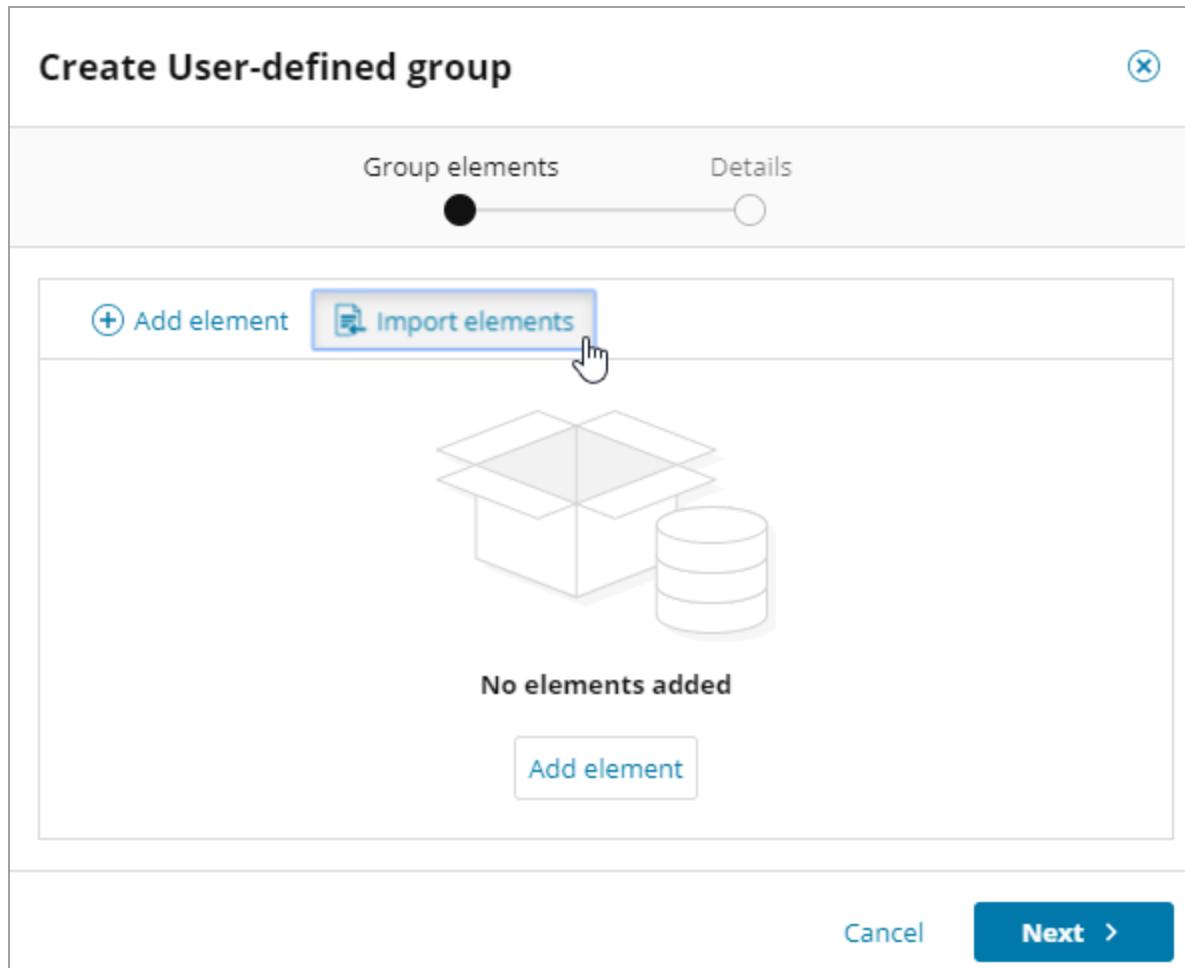
A name and value are required for each element. The asterisk (*) wildcard symbol can be used in values, if appropriate. You can add an optional description for each element.

The CSV file must begin with the Name, Value, Description header. For example:

```
Name,Value,Description
Administrators,Administrators, Top level administrators only
Backup Operators,backup oper*,
DNS Admins,DNSAdmin*,
Domain Admin,domain admin*,
```

 Importing elements will not overwrite an existing element list in a user-defined group. Imported elements are added to the list, and duplicate elements are skipped.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > User defined groups.
3. On the toolbar, click Create User-defined group or select an existing user-defined group and click Edit.
4. Click Import elements, navigate to your CSV file, and then click Open.



 The CSV file must include populated Name and Value columns. The Description column is optional.

5. Click Next.
6. Follow the instructions in the proceeding windows to complete the import.

Export user-defined group elements

1. Log in to the SEM Console.
2. On the toolbar, click Configure > User defined groups.
3. On the toolbar, click Create User-defined group, or select an existing user-defined group and click Edit.
4. Click Export elements. The CSV file downloads to your local system.

Create User-defined group

Group elements Details

+ Add element Import elements Export elements

☐ ↑ Name Search...

☐	admin	"admin"

Cancel Next >

5. Click Next.
6. Follow the instructions in the proceeding windows to complete the export.

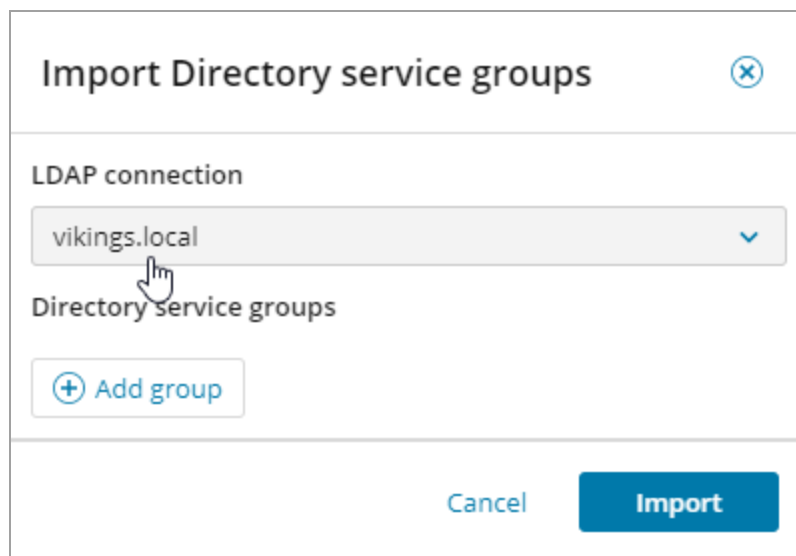
Configure directory service groups in SEM

Perform the following steps to select the Active Directory groups to synchronize with SEM. If the connector is running, the synchronization process runs every five minutes.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Directory Service Groups.
3. Click Import Directory service group.

The Import Directory service groups dialog is displayed.

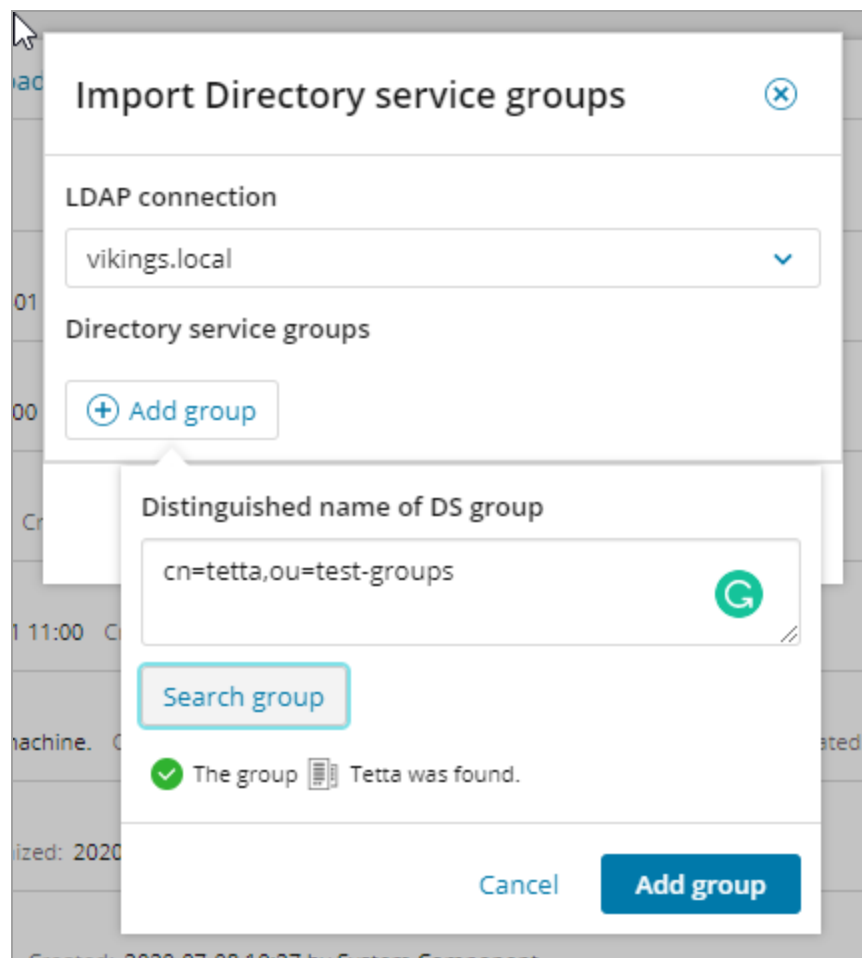
4. Click the drop-down menu and select the [LDAP configuration](#) to use.



The screenshot shows a dialog box titled "Import Directory service groups". It contains a section for "LDAP connection" with a dropdown menu currently set to "vikings.local". Below this is a section for "Directory service groups" which includes a button with a plus icon and the text "Add group". At the bottom of the dialog are two buttons: "Cancel" and "Import".

5. Click Add Groups.

A dialog window opens where you can enter the Distinguished Name (DN) of the directory service group you want to add.

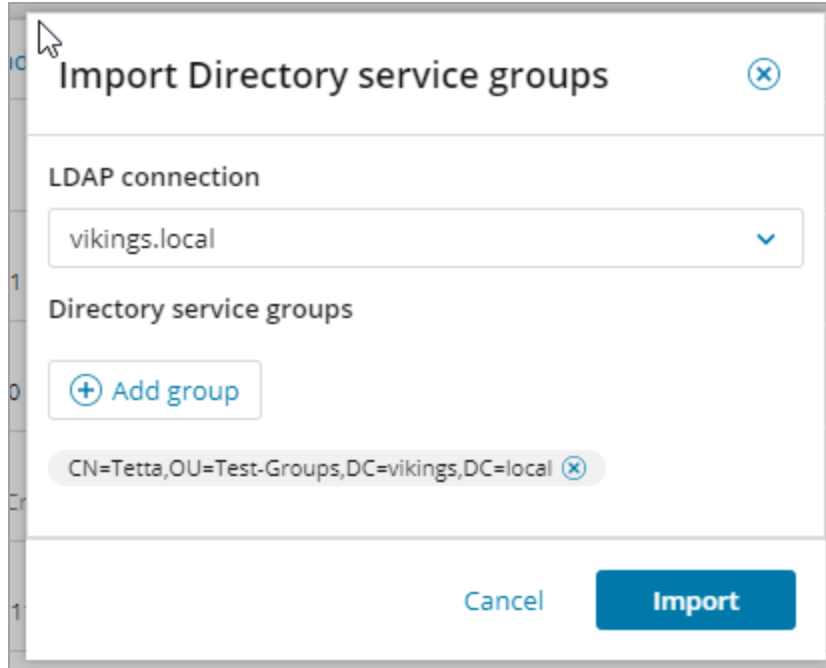


For example:

cn=A-group, ou=support, dc=mycompany, dc=com.

6. Click Search group to verify the group exists.

7. If the group is found, click Add group.



8. If you want to import further groups, repeat step 5 through step 7.
9. Click import.

View a directory service group member

The Directory service groups page lists all group synchronized with SEM. Select a DS group to view the members of that group.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Directory service groups.
3. Select the targeted group checkbox, and then click Show members.

The Show members window displays with a list of group members.

Remove a directory service group

The Directory service groups page lists all group synchronized with SEM. To remove a service group, perform the following steps:

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Directory Service Groups..

3. Select the targeted group checkbox, and then click Delete.

The Directory Service Group is removed from the SEM Console.

Create event groups

SEM includes several predefined event groups, such as virus and scanner events, process start and stop events, change management events, and so on. Event groups allow you to group together several events into a specific category to initiate a specific event filter, rule, or condition.

You can [create an event group](#) that includes a custom family of alerts, save them as an event group, and associate the groups with your rules and filters. For example, you can create an event group for events that trigger the same response from SEM. If an event in the group occurs, SEM fires the rule for that group.

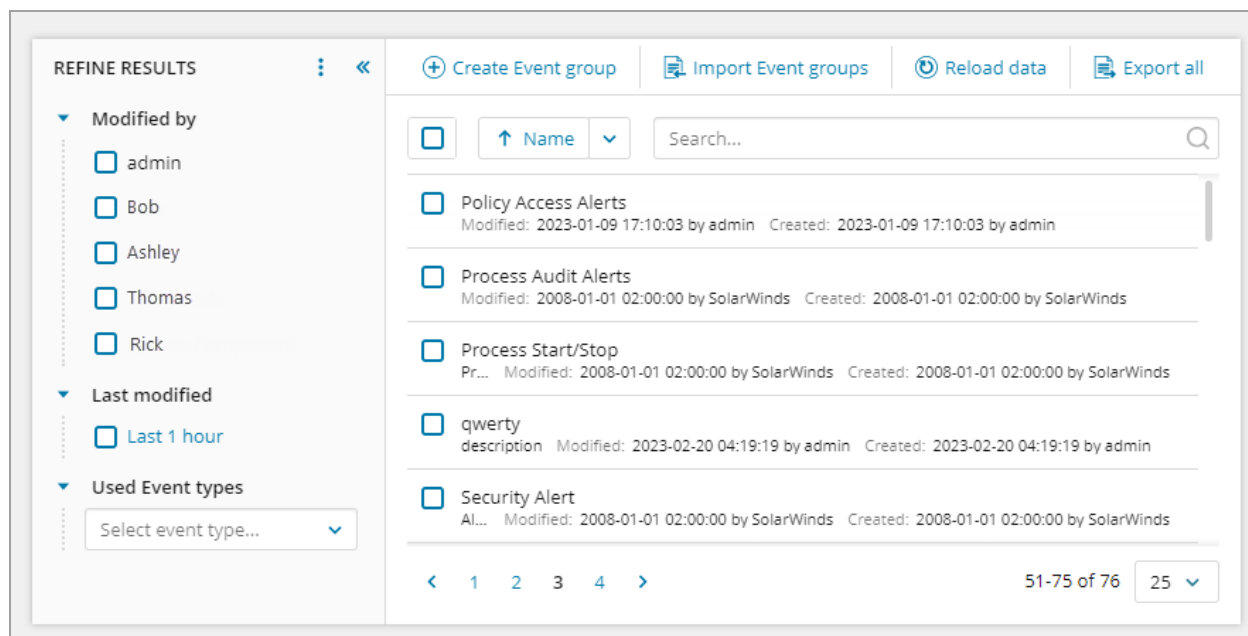
If you have multiple SEM instances, you can [import an event group](#) from another SEM instance or [export one or more event groups](#) in JSON format to another SEM instance.

 When you click Reload data or navigate to another section in the application, all selected filters, search input, pagination, and sorting settings are preserved.

Event Groups window

Click Configure > Event Groups in the SEM toolbar to access the Event Groups window.

This window displays all existing event groups. Click the ellipsis  icon to expand or collapse all refined results in the left column.



The screenshot shows the 'Event Groups' window. On the left, under 'REFINE RESULTS', there are three sections: 'Modified by' with checkboxes for admin, Bob, Ashley, Thomas, and Rick; 'Last modified' with a checkbox for 'Last 1 hour'; and 'Used Event types' with a dropdown menu. The main content area has a toolbar with '+ Create Event group', 'Import Event groups', 'Reload data', and 'Export all'. Below the toolbar is a search bar and a list of event groups. Each group has a checkbox, a name, and a description. The groups listed are: 'Policy Access Alerts' (Modified: 2023-01-09 17:10:03 by admin, Created: 2023-01-09 17:10:03 by admin), 'Process Audit Alerts' (Modified: 2008-01-01 02:00:00 by SolarWinds, Created: 2008-01-01 02:00:00 by SolarWinds), 'Process Start/Stop' (Modified: 2008-01-01 02:00:00 by SolarWinds, Created: 2008-01-01 02:00:00 by SolarWinds), 'qwerty' (Modified: 2023-02-20 04:19:19 by admin, Created: 2023-02-20 04:19:19 by admin), and 'Security Alert' (Modified: 2008-01-01 02:00:00 by SolarWinds, Created: 2008-01-01 02:00:00 by SolarWinds). At the bottom, there is a pagination bar showing '51-75 of 76' and a dropdown for '25'.

The following table describes the selectable items in the window.

Selection	Description
Modify by	Filters the event group results based on your user selections.
Last modified	Filters the event group results based on the selected time span. For example, all event groups that were modified in the last hour.
Used Event types	Filters the event group results based on your selected event types.
Create Event group	Creates a new event group based on your selected events.
Import Event groups	Imports a saved event group from another SEM instance.
Reload data	Refreshes the Event Groups window. When you click this option and navigate to another section in the application, all selected filters, search inputs, pagination, and sorting settings are preserved.
Export all	Exports all event groups to a JSON file for import to another SEM instance.
Search	Filters the event group results based on your search parameters.

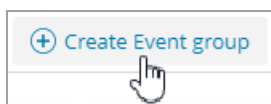
Using the Event Groups window, you can:

- [Create, edit, copy, or delete](#) an event group.
- [Export an event group](#) to another SEM instance.
- [Import an event group](#) from another SEM instance.

Create an event group

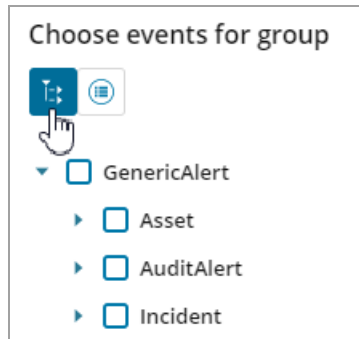
This procedure describes how to create an event group for your SEM instance.

1. In the SEM toolbar, click Configure > Event Groups.
2. Click Create event group.

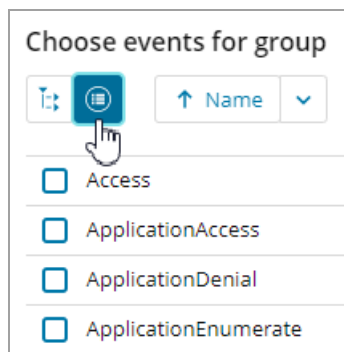


3. In the Create event group window, select the events for your new group, and then click Next.

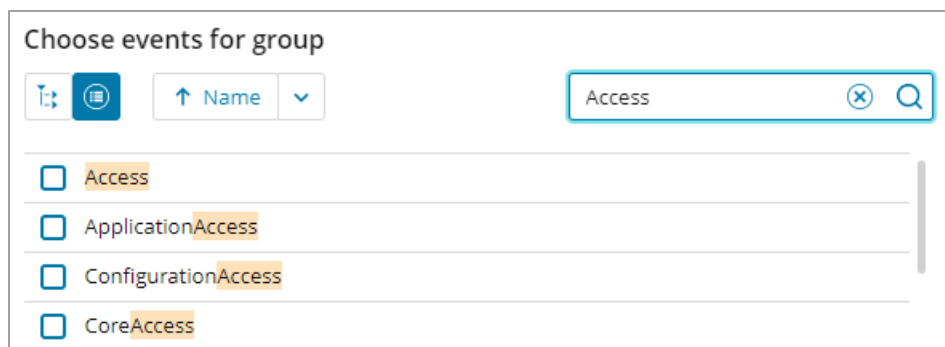
Click the tree view  icon to select a parent event and specific child events. Click Show selected only to view your selected events.



Click the list view  icon to select the targeted events and all related child events. After you select your targeted events, you can click the tree view to view all related child events.



To search for a specific event name, enter the name in the Search field and click the magnifying glass. The search results highlight all events that contain your search parameters. When you are finished, select the events you want to include in the group.



4. Under Details, enter a name and optional description for this group, and then click Create.

Details

Event group name

Description (optional)

The new event group is added to the Event Group page. Click Reload data to refresh the list.

☐ Asset and Audit Alerts
 All asset and audit alerts. Modified: 2023-02-22 14:46:05 by admin Created: 2023-02-22 14:46:05 by admin

 All selected filters, search input, pagination, and sorting settings are preserved after you click Reload data or navigate to another area and back in the application.

Edit an event group

This procedure explains how to edit an event group in your SEM instance.

1. In the SEM toolbar, click Configure > Event Groups.
2. Select the checkbox next to the event group you want to edit.

☒ Asset and Audit Alerts
 All asset and audit alerts. Modified: 2023-02-22 14:46:05 by admin Created: 2023-02-22 14:46:05 by admin

3. In the toolbar, click Edit.



4. Edit your selections in the tree or list view.

Click the tree view  icon to display a list of existing events and their corresponding child events. Select or remove additional events as required. Click the maximize arrow to view child events.

Choose events for group

☒ Show selected only

☒
☐

☒ GenericAlert

- ▶ ☒ Asset
- ▶ ☒ AuditAlert
- ▶ ☐ Incident
- ▶ ☐ InternalAlert
- ▶ ☐ SecurityAlert

Click the list view  icon to display a list of existing events that automatically include all child events. Select or remove additional events as required.

Choose events for group

☒ Show selected only

☐
☒

☐ Access

☐ ApplicationAccess

☐ ApplicationDenial

☐ ApplicationEnumerate

☒ ApplicationTrafficAudit

☒ Asset

☒ AssetManagement

☒ AssetScanResult

☐ AttackBehavior

☒ AuditAlert

- Click Next.
- Update the event group name and description as required.

Details

Event group name

Description (optional)

7. Click Save.

The edited group displays in the Event Group page.

☐ Asset, Audit, and Access Alerts
 All asset, audit, and access alerts. Modified: 2023-02-22 15:19:01 by admin Created: 2023-02-22 15:19:01 by admin

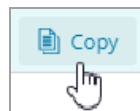
Copy an event group

This procedure explains how to copy an event group in your SEM instance. When you are finished, you can edit the event group and add or remove events from the group.

1. In the SEM toolbar, click Configure > Event Groups.
2. Select the checkbox next to the event group you want to copy.

☒ Asset, Audit, and Access Alerts
 All asset, audit, and access alerts. Modified: 2023-02-22 15:19:01 by admin Created: 2023-02-22 15:19:01 by admin

3. Click Copy.



The copied event displays in the window.

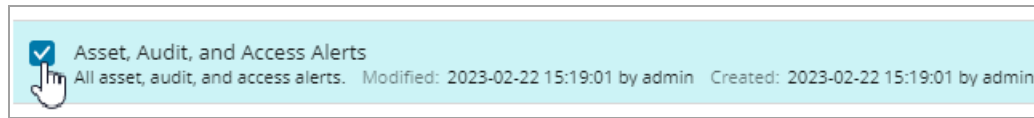
☐ Copy of Asset, Audit, and Access Alerts
 All asset, audit, and access alerts. Modified: 2023-02-22 15:43:26 by admin Created: 2023-02-22 15:43:26 by admin

4. [Edit the event group](#) as required.

Export an event group

This procedure explains how to export an existing event group in JSON format from your SEM instance to another instance.

1. In the SEM toolbar, click Configure > Event Groups.
2. Select the checkbox next to the event groups you want to export.



To export all event groups, leave all event groups unselected.

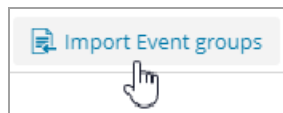
3. Click Export Event groups.

The selected event groups are exported to a JSON file and downloaded to the host server.

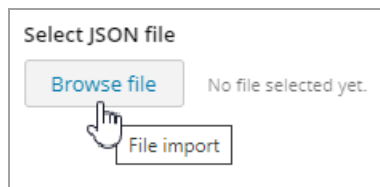
Import an event group

This procedure explains how to import an event group in JSON format from another SEM instance.

1. In the SEM toolbar, click Configure > Event Groups.
2. In the toolbar, click Import Event groups.



3. In the Import Event Groups window, click Browse file.



4. Select the event group file in JSON format to import, and then click Open.

If the file is not identical to the parent SEM instance, a warning message displays in the window. Click Browse file and select the correct file.

If the file does not include invalid event groups, no warning message displays. Click Import to complete the procedure.

If the file includes invalid event groups, do the following:

- a. Search and deselect any event groups that you do not want to import. Click the Name drop-down menu to display the list in ascending or descending order.
- b. Click Import.
- c. In the Conflicts window, select how SEM should handle the conflicts for each event group.

Select Skip to ignore the conflict.

Select Overwrite to overwrite the existing event groups with the imported event group.

Select Rename to rename the event group.

d. Click Import.

The Import Results window displays the actions you selected to resolve the conflicts in each event group.

Troubleshoot importing an event group

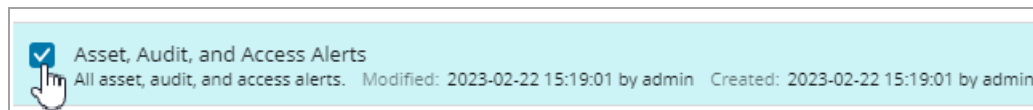
The following table provides workarounds for importing an event group.

Error message	Action
File is too large to upload. The maximum supported file size is 2 MB.	Modify the file so it is smaller than 2 MB. You can split the file into several files.
Invalid content. Uploaded file should have the same format as exported file.	Modify the file so it has the correct formatting. You can export another event group, compare the structure with your new event group, and then export the file.
File empty. Selected file is empty. Upload a JSON file containing SEM Event Groups.	Modify the file so it has the correct data and formatting.
Invalid event groups. <X> of <x> event groups are invalid. These event groups cannot be imported.	Modify the file so it has the correct data. Error messages in the list records (such as "invalid name" or "invalid members" can help you identify the issue.

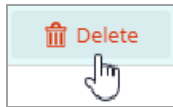
Delete an event group

This procedure explains how to delete an event group from your SEM instance.

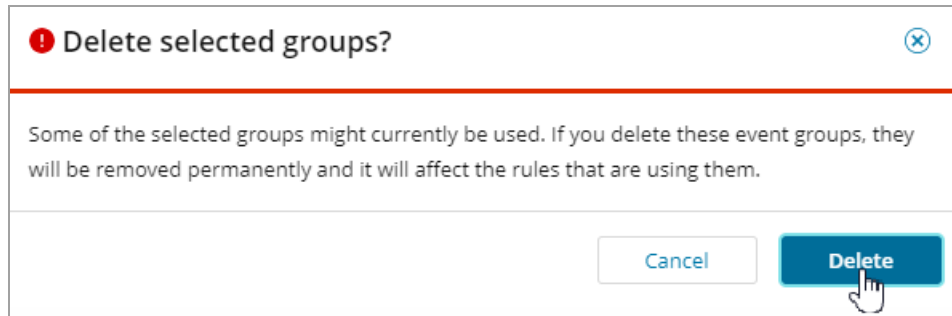
1. In the SEM toolbar, click Configure > Event Groups.
2. Select the checkbox next to each event group you want to delete.



3. In the toolbar, click Delete.



4. In the dialog box, click Delete.



The selected event groups are deleted.

Create time of day groups

Time of day groups are groups of hours that you associate with rules and filters to execute different actions at different times of the day. You can create as many groups as required to reflect your business needs. A well-planned set of groups provide you with versatile and responsive rules that perform the way you want and when you want.

For example, if you [create time of day groups](#) for both normal and after business hours, you can assign separate rules to each group. For normal business hours, you can [create a new rule](#) to alert your system administrator using email. For after business hours, you can assign a rule to alert a night shift administrator and automatically shut down the offending system.

i Each group you create only applies to the manager you select when you create the group. If you need a similar group for another manager, create it separately with the alternate manager.

SEM includes out-of-the-box group templates that are highlighted with the icon, as shown below. You can modify these templates, but they cannot be deleted.

REFINE RESULTS

Modified by

☐ admin
 ☐ ekoc
 ☐ SolarWinds

Last modified

☐ Last 1 hour

+

 Create Time of day group

Import Time of day groups

Reload data

Export all

☐

↑ Name

↓

Search...

☐ Early Shift

Early Shift

Modified: 2008-01-01 02:00:00 by SolarWinds Created: 2008-01-01 02:00:00 by SolarWinds

☐ Graveyard Shift

Graveyard Shift

Modified: 2008-01-01 02:00:00 by SolarWinds Created: 2008-01-01 02:00:00 by SolarWinds

☐ Late Shift

Late Shift

Modified: 2008-01-01 02:00:00 by SolarWinds Created: 2008-01-01 02:00:00 by SolarWinds

☐ Normal Shift

Modified: 2020-04-02 05:48:36 by admin Created: 2008-01-01 02:00:00 by SolarWinds

☐ Reboot Cycle

Modified: 2008-01-01 02:00:00 by SolarWinds Created: 2008-01-01 02:00:00 by SolarWinds

<

1

2

>

1-25 of 36

25

Filter the group menu

The **Modify by** options in the Refined Results column filters and displays only those groups last modified by a specific role or user. For example, when you click the SolarWinds checkbox, the console displays the group templates modified by SolarWinds and included with the application.

Click  to expand or collapse the menu options.

REFINE RESULTS

Modified by

☐ admin
 ☐ admin
 ☐ admin1
 ☐ ekoc
 ☐ ppaim
 ☒ SolarWinds

Last modified

☐ Last 1 hour

+

 Create Time of day group

Import Time of day groups

Reload data

Export filtered

☐

↑ Name

↓

Search...

☐ Graveyard Shift

Graveyard Shift

Modified: 2008-01-01 02:00:00 by SolarWinds Created: 2008-01-01 02:00:00 by SolarWinds

☐ Late Shift

Late Shift

Modified: 2008-01-01 02:00:00 by SolarWinds Created: 2008-01-01 02:00:00 by SolarWinds

☐ Reboot Cycle

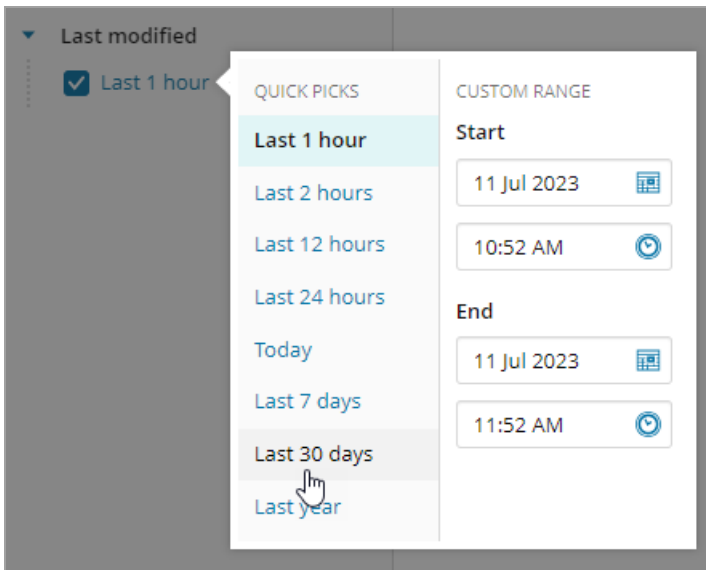
Modified: 2008-01-01 02:00:00 by SolarWinds Created: 2008-01-01 02:00:00 by SolarWinds

The **Last modified** option filters all groups that were last modified within a specific timeframe. The default selection allows you to list all groups that were modified in the last hour. To select another timeframe, click the last modified link and select a new timeframe.

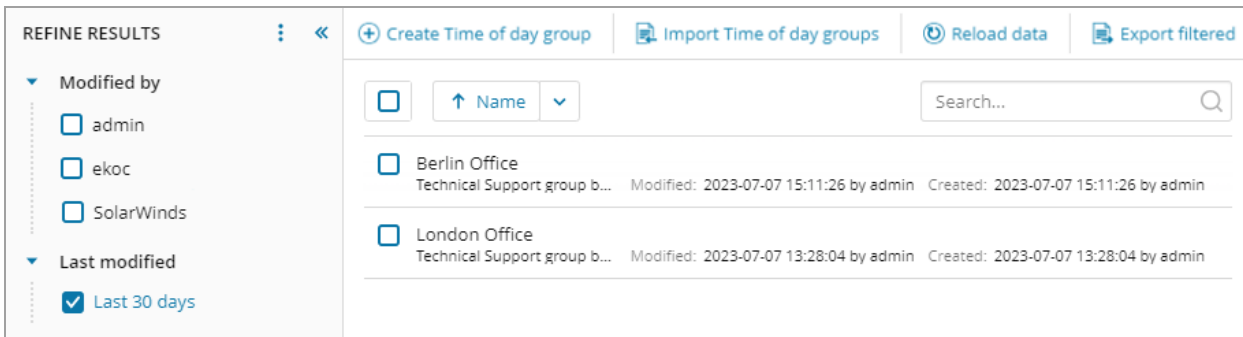
For example, you want to view all groups that were modified in the last 30 days. To select this timeframe, click the last modified link (for example, Last 1 hour) and click Last 30 days in the Quick Picks menu.

Administrator Guide: Security Event Manager

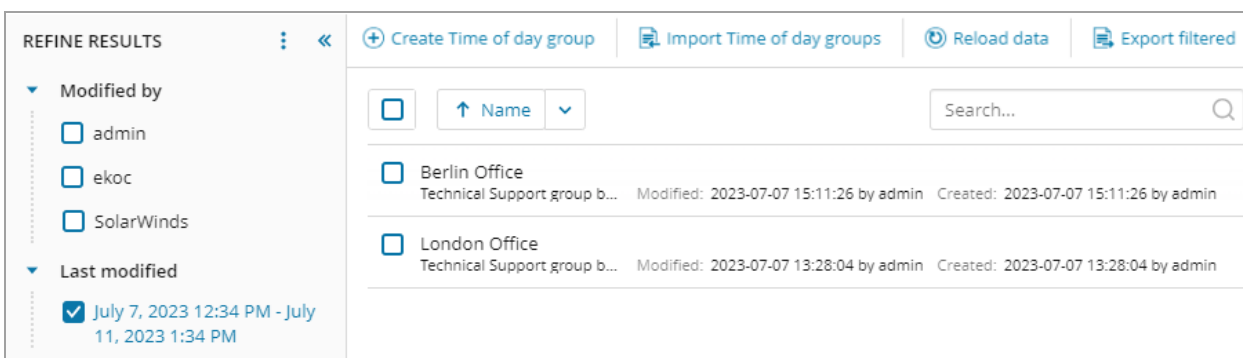
page 281



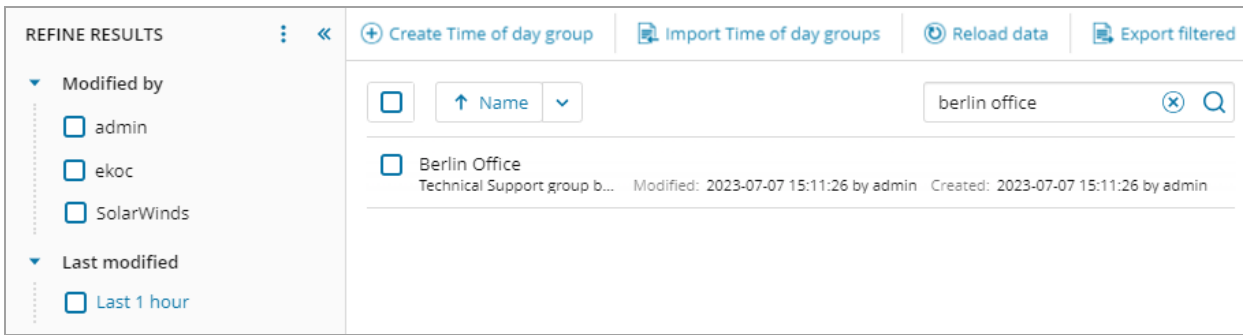
When you are finished, the console displays all groups that were last modified in the last 30 days.



If you selected a custom range for your last modified date, the selected range displays as your Last modified selection.



To **search** for a group name, enter a search term in the Search field, and then click  to display the results in the console.

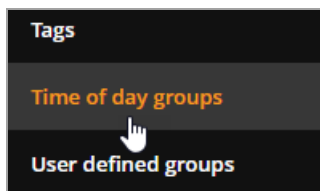


Create a group

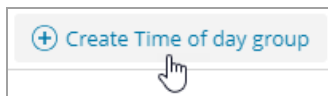
You can create a time of day group for a [specific time frame](#) or a [continuous time span](#). When required, you can [edit, delete](#), or [copy](#) a time of day group.

Create a group with a specific time frame

1. Log in to the SEM Console as an administrator.
2. In the toolbar, click Configure > Time of day groups.



3. In the toolbar, click Create Time of day group.



4. In the Create time of day group grid, define the daily timeslots when the SEM Manager enables a rule or filter for the time of day group.

- a. In the grid, click the hour when the first timeslot begins (for example. Monday at 08:00). Do not release the mouse button.

Choose time of day for group

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
08:00	08:00						
09:00							
10:00							
11:00							
12:00							

- b. Drag the mouse arrow to the hour when this timeslot ends (for example, Monday at 12:00), and then release the mouse button.

Choose time of day for group

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
08:00	08:00						
09:00							
10:00							
11:00							
12:00	12:00						

- c. Click the selected timeslot.
- d. In the pop-up menu, clone the selected timeslot to additional week days that apply to this group.

Choose time of day for group

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
08:00	08:00	08:00	08:00	08:00	08:00		
09:00							
10:00							
11:00							
12:00	12:00				12:00		

Time: 08:00 - 12:00

Mo Tu We Th Fr Sa Su

☒ ☒ ☒ ☒ ☒ ☐ ☐

- e. When you are finished, press <Esc> to hide the pop-up menu.

Choose time of day for group

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
08:00	08:00	08:00	08:00	08:00	08:00		
09:00							
10:00							
11:00							
12:00	12:00	12:00	12:00	12:00	12:00		

- f. (Optional) Drag the top or bottom edge of one or more timeslots to modify the time range for a specific day.

Choose time of day for group

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
08:00	08:00	08:00	08:00	08:00	08:00		
09:00							
10:00							
11:00					11:00		
12:00	12:00	12:00	12:00	12:00			

g. Click Next.

5. Enter a group name and an optional description.

For example:

Create time of day group

Choose time of day

Details

Details

Time of day group name

London Office

Description

Technical Support group based in London.

Cancel

< Back

Create

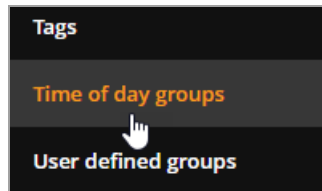
6. Click Create.

The new time of day group is added to the Time of day group page.

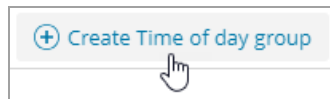
☐ London Office Technical Support group based in London. Modified: 2023-07-07 13:28:04 by admin Created: 2023-07-07 13:28:04 by admin

Create a group with a continuous timespan

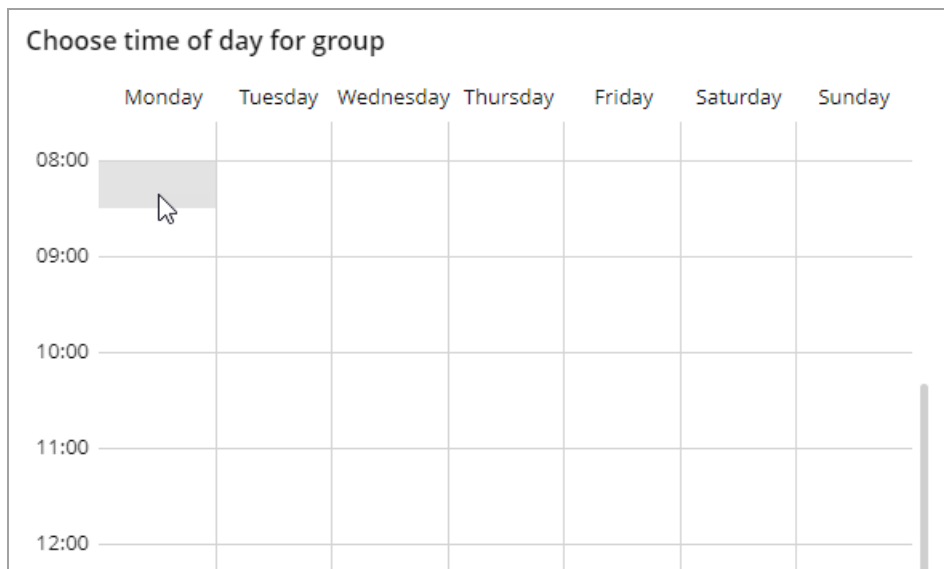
1. Log in to the SEM Console as an administrator.
2. In the toolbar, click Configure > Time of day groups.



3. In the toolbar, click Create Time of day group.

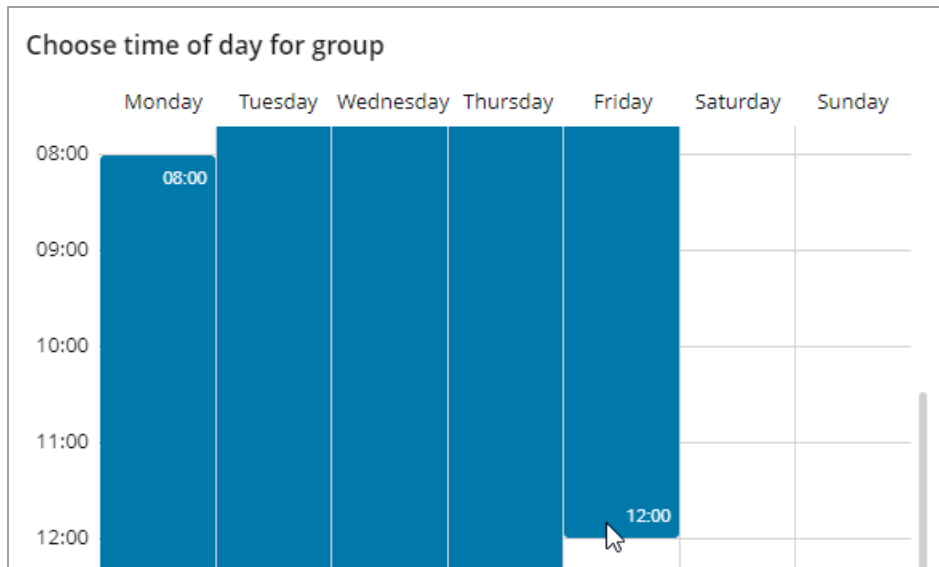


4. In the Create time of day group grid, define the 24-hour time span when the SEM Manager enables a rule or filter for the time of day group.
 - a. In the grid, click the hour when the first timeslot begins (for example, Monday at 08:00). Do not release the mouse button.



- b. Drag the mouse arrow to the day and hour when this timeslot ends (for example, Friday at

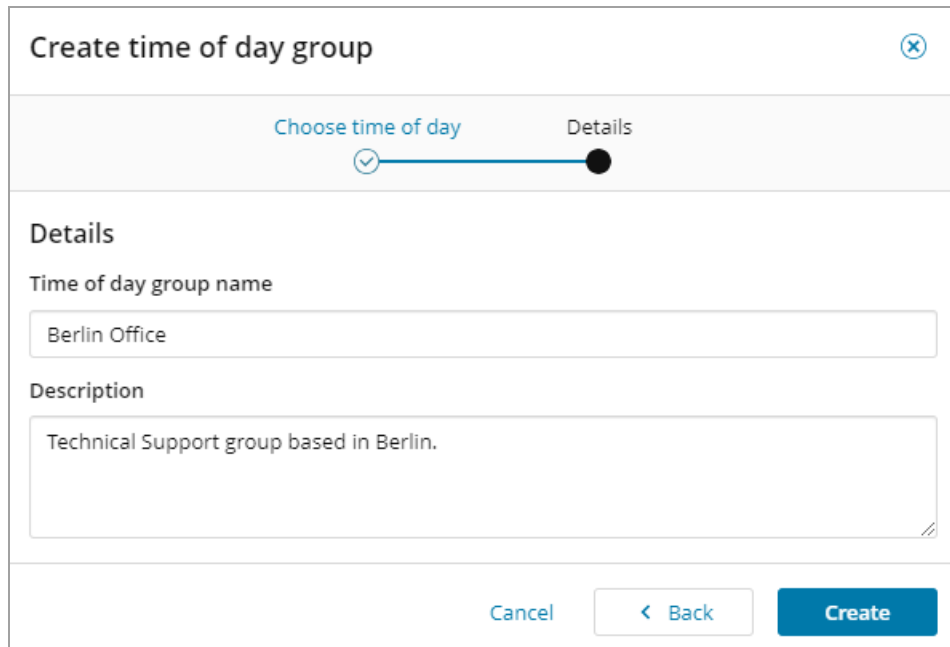
12:00), and then release the mouse button.



c. Click Next.

5. Enter a group name and an optional description.

For example:



The screenshot shows the 'Create time of day group' dialog box. The 'Details' tab is active, showing fields for 'Time of day group name' (Berlin Office) and 'Description' (Technical Support group based in Berlin.). Navigation buttons 'Cancel', '< Back', and 'Create' are at the bottom.

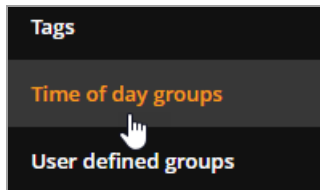
6. Click Create.

The new time of day group is added to the Time of day group page.

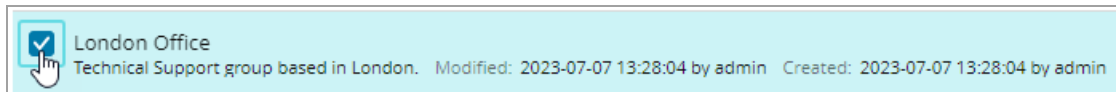
☐	Berlin Office	Technical Support group based in Berlin.	Modified: 2023-07-07 15:11:26 by admin	Created: 2023-07-07 15:11:26 by admin

Edit a group

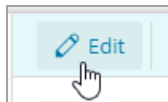
1. Log in to the SEM Console as an administrator.
2. In the toolbar, click Configure > Time of day groups.



3. Select the time of day group you want to edit.

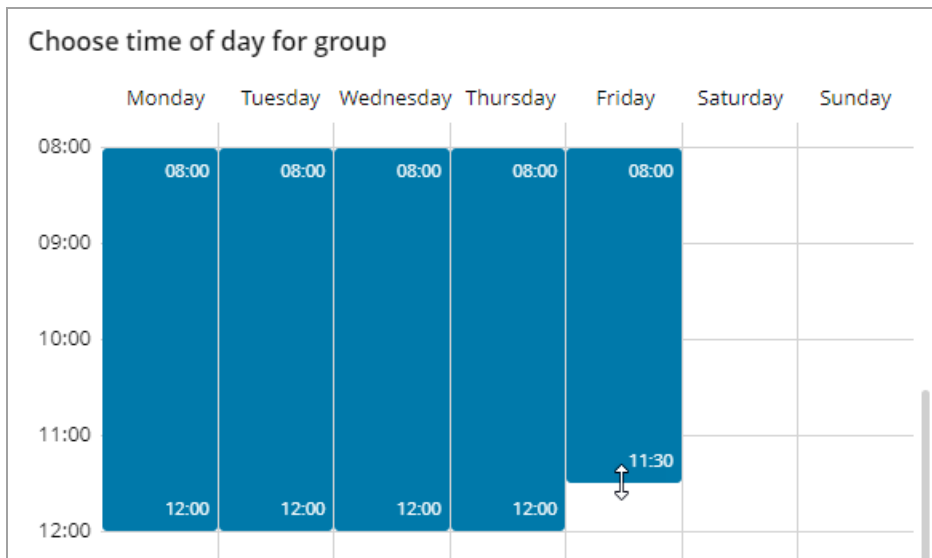


4. In the toolbar, click Edit.



5. Edit the timeslots as required.

To change the timeslot for each day, drag the top or bottom timeslot edge to a new hour.



To add or remove days of the week, click a timeslot and select or deselect the targeted days of the week. When you are finished, click a timeslot to hide the pop-up menu.

Choose time of day for group

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
08:00	08:00	08:00	08:00	08:00			
09:00							
10:00							
11:00							
12:00	12:00	12:00	12:00	12:00			

Time: 08:00 - 12:00

Mo	Tu	We	Th	Fr	Sa	Su
☒	☒	☒	☒	☐	☐	☐

- Click Next.
- Verify that the group name and description is correct, and then click Save.

Edit time of day group - London Office

Choose time of day ☒ Details ☐

Details

Time of day group name

London Office

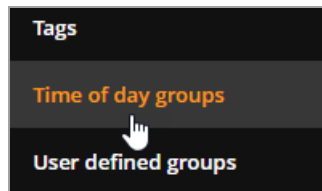
Description

Technical Support group based in London.

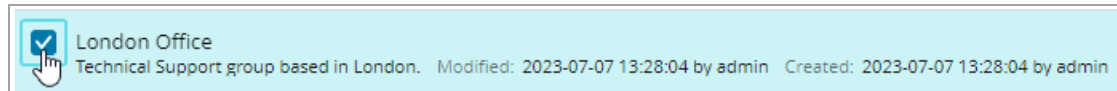
Cancel [< Back](#) [Save](#)

Delete a group

- Log in to the SEM Console as an administrator.
- In the toolbar, click Configure > Time of day groups.



3. Select the time of day group you want to delete.

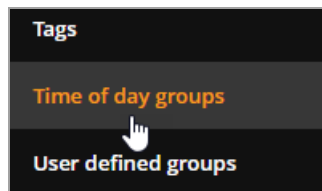


4. In the toolbar, click Delete.

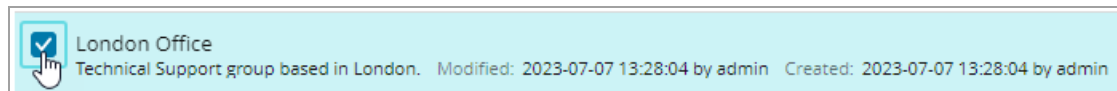


Copy a group

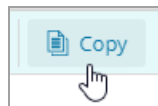
1. Log in to the SEM Console as an administrator.
2. In the toolbar, click Configure > Time of day groups.



3. Select the time of day group you want to delete.



4. In the toolbar, click Copy.



View live and historical events

This section describes the historical and live events and how to set up, manage, and import or export queries and filters.

Live Events view

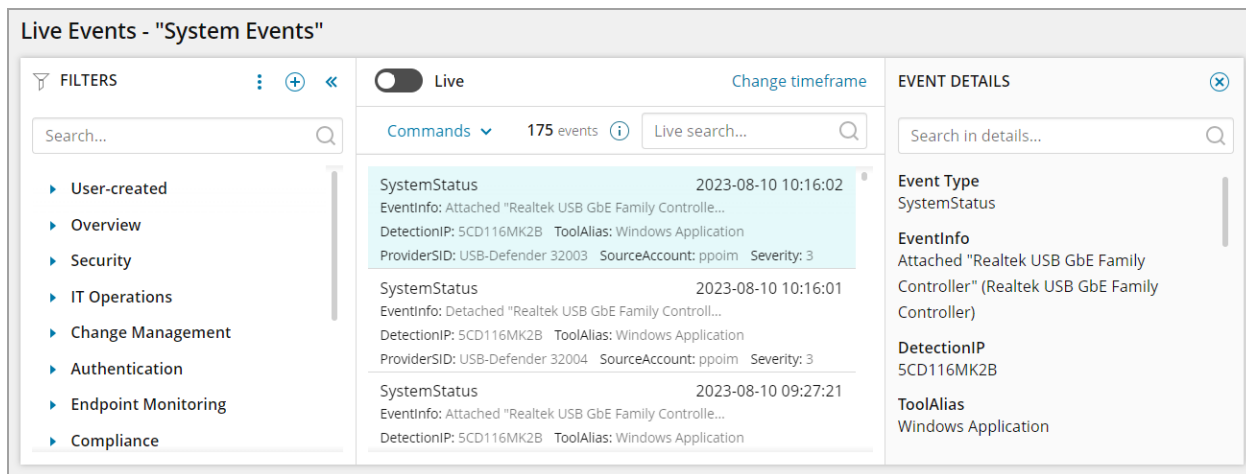
See [About the event types](#) for descriptions of all events and their corresponding alerts.

The SEM console provides instant access to live event monitoring and filtering, as well as [historical record data](#) for in-depth analysis and troubleshooting. Within the console view, you can quickly switch between real-time event streaming and historical log views based on user-defined date and time parameters.

The Live Events screen displays all live event data that is passing through a particular SEM Manager instance. Use this screen to view real-time events as they occur in your deployment.

Live Events screen

Log in to the SEM console and click Live Events in the toolbar. The following example displays the event results for a selected event (highlighted in blue).



Live Events - "System Events"

FILTERS + « Live Change timeframe

Search...

- ▶ User-created
- ▶ Overview
- ▶ Security
- ▶ IT Operations
- ▶ Change Management
- ▶ Authentication
- ▶ Endpoint Monitoring
- ▶ Compliance

Commands 175 events Live search...

SystemStatus	2023-08-10 10:16:02
EventInfo: Attached "Realtek USB GbE Family Controll...	
DetectionIP: 5CD116MK2B ToolAlias: Windows Application	
ProviderSID: USB-Defender 32003 SourceAccount: ppolm Severity: 3	
SystemStatus	2023-08-10 10:16:01
EventInfo: Detached "Realtek USB GbE Family Controll...	
DetectionIP: 5CD116MK2B ToolAlias: Windows Application	
ProviderSID: USB-Defender 32004 SourceAccount: ppolm Severity: 3	
SystemStatus	2023-08-10 09:27:21
EventInfo: Attached "Realtek USB GbE Family Controll...	
DetectionIP: 5CD116MK2B ToolAlias: Windows Application	

EVENT DETAILS ×

Search in details...

Event Type
SystemStatus

EventInfo
Attached "Realtek USB GbE Family Controller" (Realtek USB GbE Family Controller)

DetectionIP
5CD116MK2B

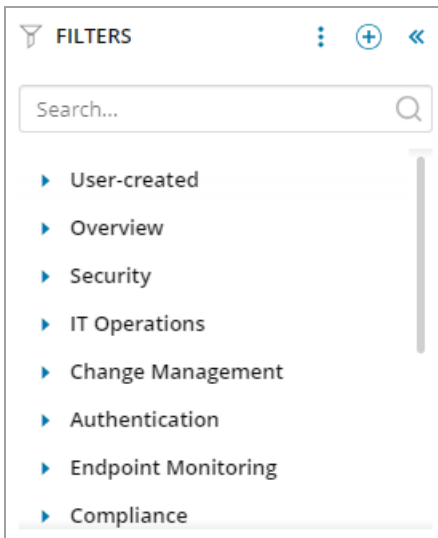
ToolAlias
Windows Application

The Live Events view consists of three panes:

- [Filters](#)
- [Events](#)
- [Event Details](#)

Filters

The Filters pane displays the filters you can apply to the event messages. Click the Hide Pane icon » to collapse this pane. Click the Show Pane icon « to expand it.



For more information, see:

- [About SEM filters](#)
- [Create filters in SEM](#)

Events

The Events pane displays the events that exist for your selected filter. The title bar displays the name of the filter currently selected in the Filters pane. Enter an event name in the Search field and then click the magnifying glass icon to locate a specific event in the center column.

The following example shows all events in list view. Click Switch to table view to display all events in a table.

☒ Live
 Change timeframe

Export
Switch to table view
175 events
Live search...

SystemStatus EventInfo: Attached "Realtek USB GbE Family Controll... ToolAlias: Windows Application ProviderSID: USB-Defender 32003 SourceAccount: ppoim Severity: 3 StatusLevel: 321000001 InsertionTime: 2023-08-10 10:16:02 Manager: swi-sem StatusMessage: Realtek	2023-08-10 10:16:02
SystemStatus EventInfo: Detached "Realtek USB GbE Family Controll... ToolAlias: Windows Application ProviderSID: USB-Defender 32004 SourceAccount: ppoim Severity: 3 StatusLevel: 321000001 InsertionTime: 2023-08-10 10:16:02 Manager: swi-sem StatusMessage: Realtek	2023-08-10 10:16:01

Live mode

Within the Live Events screen, you can switch between real-time event streaming and historical log views based on user-defined date and time parameters.

Drag the switch to the right to collect all live events. The Events meter displays the number of the events that match the selected filter display as they occur.

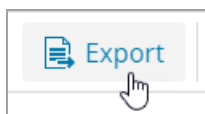


Drag the switch to the left to freeze the live events feed. The [Events meter](#) displays the number of undisplayed event messages.



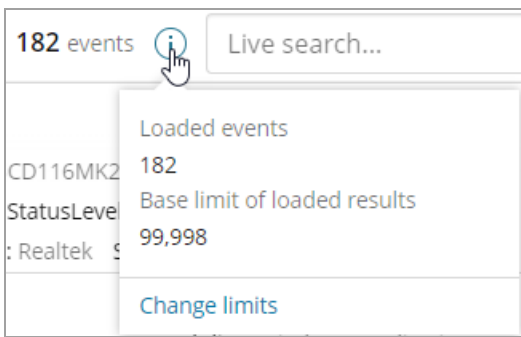
Export

Click Export to export a list of collected events to a Microsoft Excel file.



Events meter

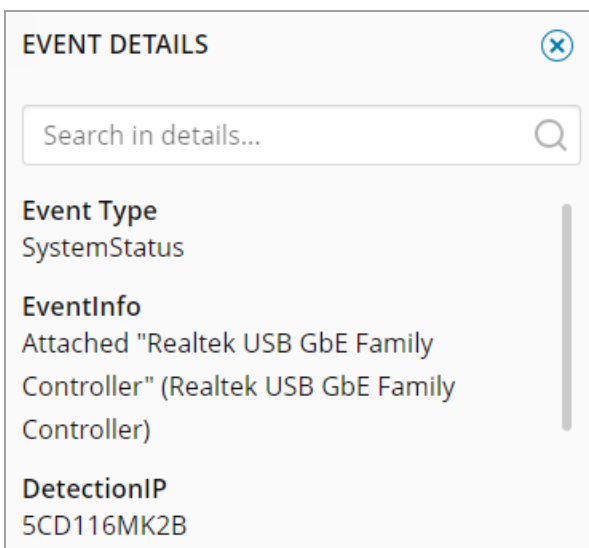
The events meter displays the number of all captured events. Click [i](#) to review the base limit setting of all loaded results.



The base limit lists the maximum number of collected events that display in the center column. See [Set live and historical event limits](#) for details on how to change the base limit.

Event Details

The Event Details pane displays information about the highlighted event in the Events table.



When you click an event, the event details display in the right column. Enter a keyword in the Search field to filter and view specific event data.

See [Filter and export event logs](#) for more information.

About SEM filters

Network activity generates events and alerts, some of which are of interest or use at any particular time. SEM filters capture and display the events and alerts that meet your specific requirements.

You can turn filters on and off, pause filters to sort or investigate events, perform actions to respond to events, and configure filters to notify you when they capture an event. Filters can also be used with dashboard widgets that display charts and graphs to visually represent the event data.

Filter conditions can be broad or specific. For example:

- The default "All" filter captures all events, regardless of the source or event type
- The filter "User Account Changes" in the Change Management group of filters, only captures one event: Auditable User Events Occurred
- The filter "FTP Traffic" in the group of filter, captures any of the following events:
 - Network Audit Alerts.EventInfo is equal to *FTP*
 - Network Audit Alerts.SourcePort is equal to 20
 - Network Audit Alerts.SourcePort is equal to 21
 - Network Audit Alerts.DestinationPort is equal to 20
 - Network Audit Alerts.DestinationPort is equal to 21

Filters and rules

Create filters when you want to group a type of event. For example, you can create filters to collect all events from your domain controllers, or all events for a specific type of user.

Create rules when you want SEM to act in response to one or more events. See [Create rules that respond to security events](#) for more information.

 Rules can be quickly created from filters as described in [Create a rule from a filter](#).

Use filters to group a type of event or to monitor specific events

You can create filters to collect all events from your firewalls, domain controllers, specific user types, and recurring, expected events.

You can also create custom filters to specific events. The following table lists the filter types you can create in SEM.

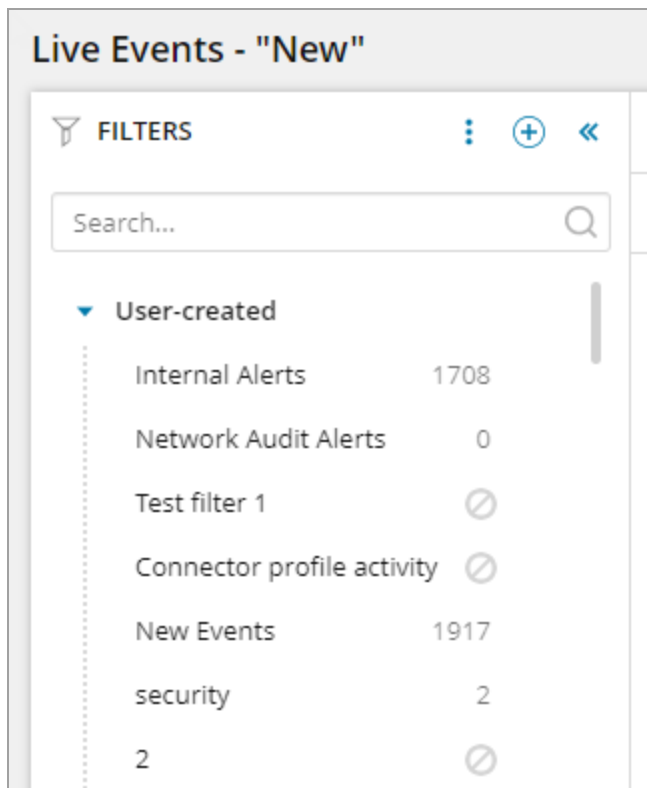
Filter type	Use
Change management filter	Monitors configuration changes users implement in your network
High volume event filter	Monitors traffic spikes or unexpected off-peak traffic.
General interest filter	Monitors logs in failures and failed authentications.  A failed authentication is an event triggered by three logon failures by the same account within an extremely short period of time.
Rule scenario event filter	Determines if you have the appropriate events to create a rule for a specific scenario.
Daily problem event filter	Monitors basic operational problems (such as account lockouts) in real time.

Default filters included with SEM

SEM includes filters that support best practices in the security industry. You can modify these filters to meet your needs, or you can create an unlimited number of custom filters. A single set of filters can monitor data collected across multiple SEM Managers.

Locate and view filters

Click the Live Events tab on the toolbar to locate a filter. Expand a category (such as Overview or IT Operations) to view its filters. The number of events that match the filter's criteria is displayed on-screen. Click a filter to display the filtered events in the log viewer table. Initially, all events are displayed.



SEM filter categories

By default, filters in the Filters pane are grouped into the following categories:

- Overview
- Security
- IT Operations
- Change Management
- Authentication
- Endpoint Monitoring
- Compliance

Learn about creating filters [here](#).

Default filters included with SEM

The following default filters are included with SEM.

Overview filters

Name	Description	Default Status
All Events	Displays all events from all sources.	On

Security filters

Name	Description	Default Status
Incidents	Filters all events categorized as Incidents.	On
Security Events	Filters events categorized as attack activity or potentially suspicious.	On
Network Event Threats	Filters events with source or destination detected in the threat intelligence feed as potentially bad actors.	On
All Firewall Events	Filters events from firewall devices that match the targeted name.	On
All Threat Events	Filters all events with the source or destination detected in the threat intelligence feed as potentially bad actors.	On
Denied ACL Traffic	Filters events from network devices that indicate denied ACL activity.	Off
Unusual Network Traffic	Filters unusual network traffic and scans.	On
Blocked Web Traffic	Filters events from proxy servers or other web servers that blocked an attempt to access a URL.	On
Proxy Bypassers	Filters web traffic users who are bypassing your proxy server.	Off
Web Traffic - Spyware	Filters web traffic events to potential spyware sites.	Off
Virus Attacks	Filters events that indicate potential virus detection.	On

Name	Description	Default Status
IDS Scan / Attack Activity	Filters security events detected by IDS tools (such as Snort).	On
Security Processes	Filters security-related process activities.	On
File Audit Failures	Filters events that indicate failed attempts to access files.	On

IT Operations filters

Name	Description	Default Status
All Domain Controller Events	Displays all traffic from machines in the Domain Controllers tool profile.	Off
All Web Traffic	Filters all web traffic-related events from network devices, proxy servers, and web servers.	On
Software Installation/Update	Filters events related to software installation and updates.	On
Service Events	Filters events related to starting and stopping services, as well as service warnings and information.	On
System Events	Filters events related to system availability and status information.	On
Error Events	Filters events from all sources that contain "error".	On
Warning Events	Filters events from all sources that contain "warning".	On
Windows Error Events	Filters events from Microsoft Windows event logs that contain "error".	On
Error Events for Device	Filters events from a specific device that contain "error".	Off
Web Traffic for Source Machine	Filters web traffic emanating from a certain source machine.	Off
All Network Traffic	Filters all network traffic-related events from all devices and systems.	On
FTP Traffic	Filters TCP traffic events between one or more FTP ports reported by any device or system.	On

Name	Description	Default Status
SNMP Traffic	Filters UDP traffic events between one or more SNMP ports reported by any device or system.	On
SMTP Traffic	Filters UDP traffic events between one or more SMTP ports reported by any device or system.	On

Change Management filters

Name	Description	Default Status
General Change Management	Filters all events that indicate changes to devices, systems, users, groups, and domains.	On
User Account Changes	Filters changes to existing user accounts.	On
Machine Account Changes	Filters changes to existing machine accounts.	On
Group Changes	Filters creation, deletion, and changes to groups.	On
Domain & Membership Changes	Filters new and deleted domain accounts (including users/groups) and domain changes.	On
Device/System Policy Changes	Filters events related to policy changes on devices and systems.	On
All File Audit Activity	Filters events related to all types of audited file access.	On
USB File Auditing	Filters file-related alerts from Agents running USB Defender	On

Authentication filters

Name	Description	Default Status
User Logons	Filters all types of user logons.	On
Interactive User Logons	Filters background network logon types.	On
Remote User Logons	Filters events that indicate remote Windows system logons.	On
Failed Logons	Filters events that indicate failed logon attempts to devices and systems.	On

Name	Description	Default Status
Account Lockouts	Filters events that indicate an account was locked out.	On
Authentication Event Threats	Filters authentication events with a source or destination detected in the threat intelligence feed as potentially bad actors.	On
Admin Account Authentication	Filters authentication events related to specified administrative accounts.	Off

Endpoint Monitoring filters

Name	Description	Default Status
Workstation Logon/Logon Failure Activity	Filters non-network workstation logon/logon failure to a domain or local account.	On
Local Account Authentication/Changes	Filters any user-related audit events that are not to or from the corporate domain.	On
Software Installed on Workstations	Filters software installations on workstation systems.	On
USB-Defender Events	Filters USB Defender events.	On
Workstation Events with Threats	Filters all events detected on endpoints with a source or destination detected in the threat intelligence feed as potentially bad actors.	On

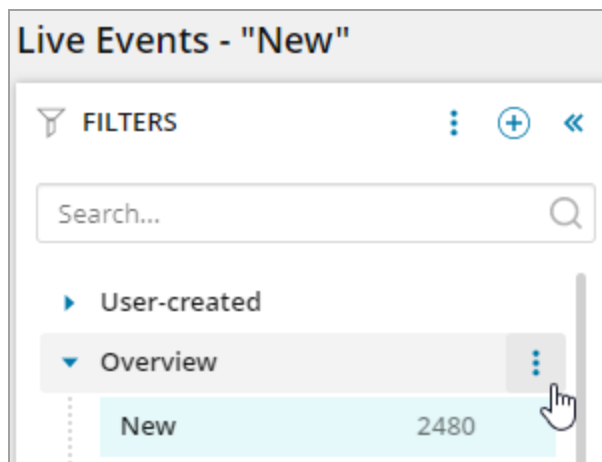
Compliance filters

Name	Description	Default Status
Top PCI Events	Filters the most common PCI events of interest, which include change management, unexpected file access, incidents, and attacks.	Off
Top HIPAA Events	Filters file activity, changes, and incidents related to HIPAA events.	Off
Top Banking Compliance Events	Filters common banking compliance events, including change management, users and groups, and potentially suspicious attack activity.	Off

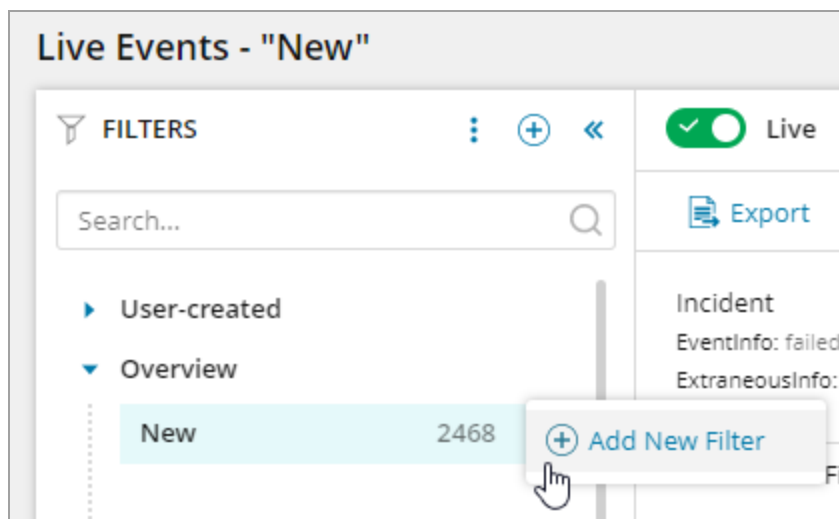
Create filters in SEM

Using the SEM Console, you can create custom filters for your event log stream to complement existing SEM filters. On the Add New Filter page, create filters by dragging and dropping default filter fields to the right side of the page, and set up values and conditions using this fields, to build a filter that determines which events are monitored.

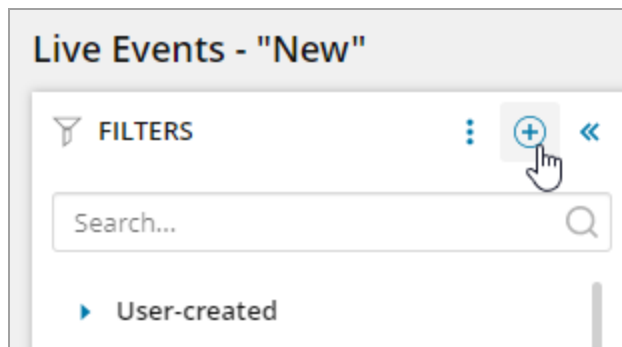
1. Log in to the SEM Console.
2. On the toolbar, click the Live Events tab.
3. To create a filter within a group, move the mouse pointer over the group heading to expose the vertical ellipsis  icon.



4. Click on the vertical ellipsis  icon and select Add New Filter.

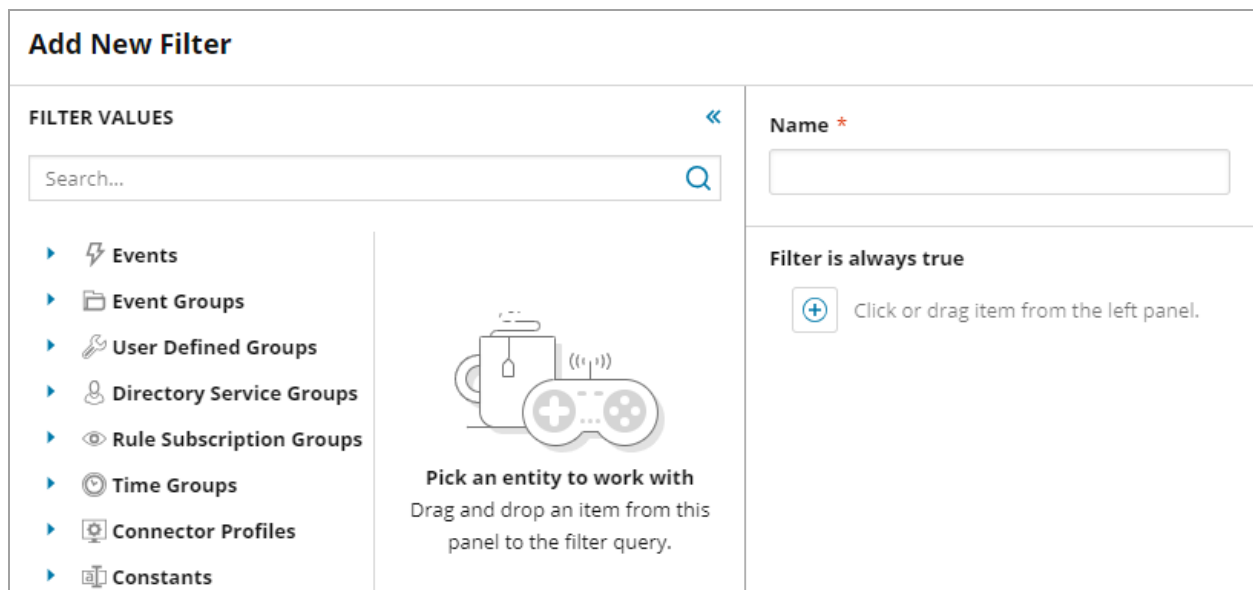


To create a filter outside of the groups, click the add  icon at the very top of the column, and select Add New Filter.



5. Enter a descriptive name for your new filter.

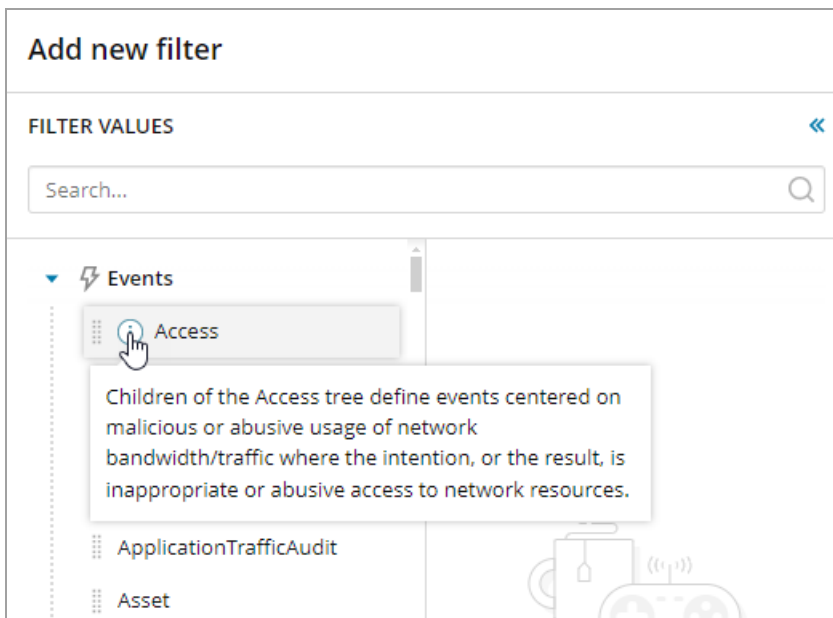
 To establish notifications for the new filter, you can [create a rule](#) based on your filter with one click.



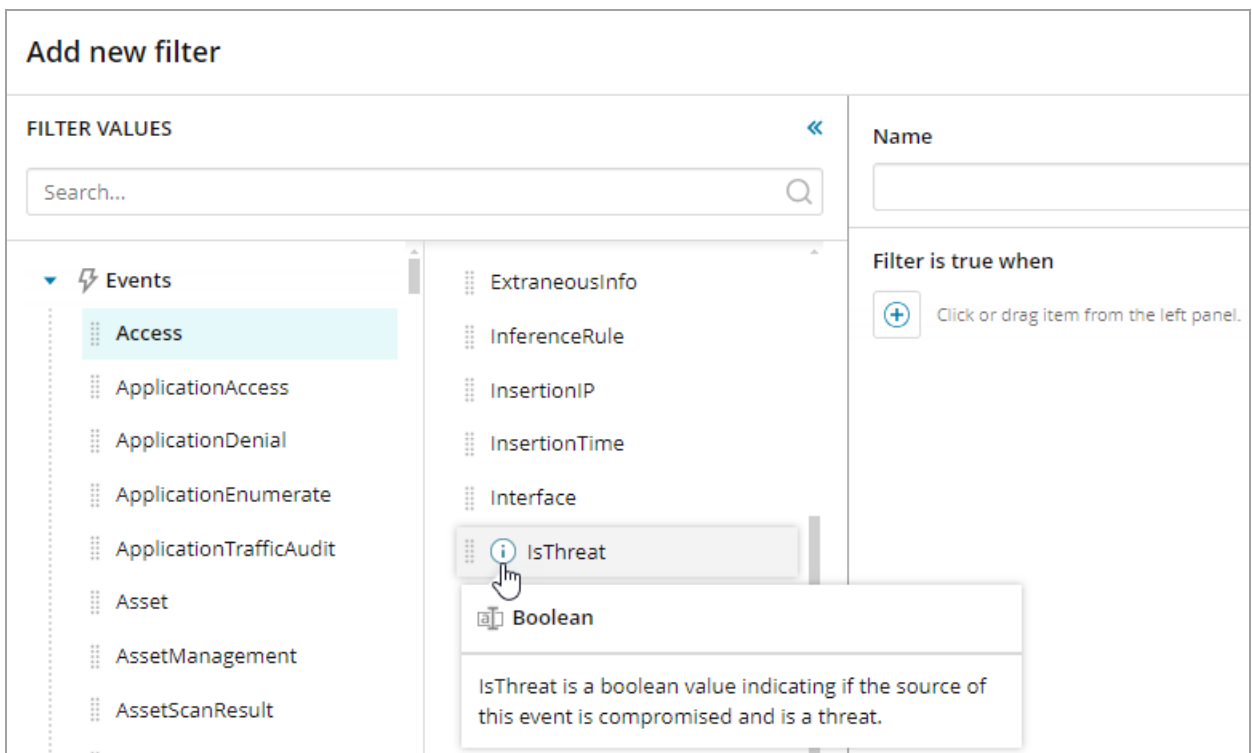
6. Add the filter fields to a filter.

- Expand Events or Event Groups to display the filter entities, and then select an entity and an optional corresponding filter.

Hover your mouse arrow over the information  icon to view a description of the entity.



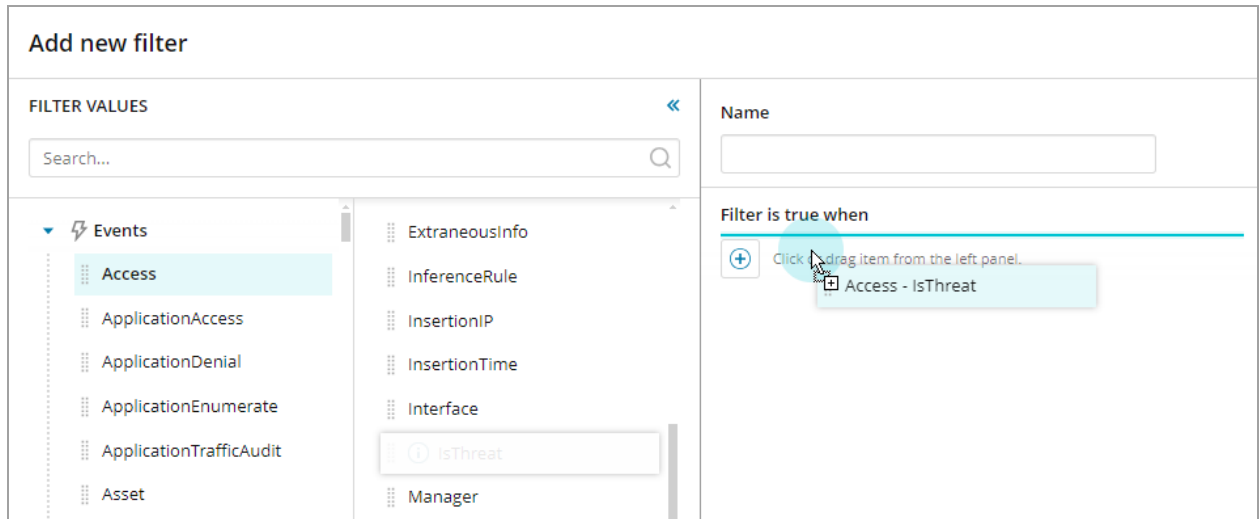
Some filter entities, such as those in the Events group, can be expanded to show filter fields. Hover your mouse arrow over the information  icon to view a description of the field.



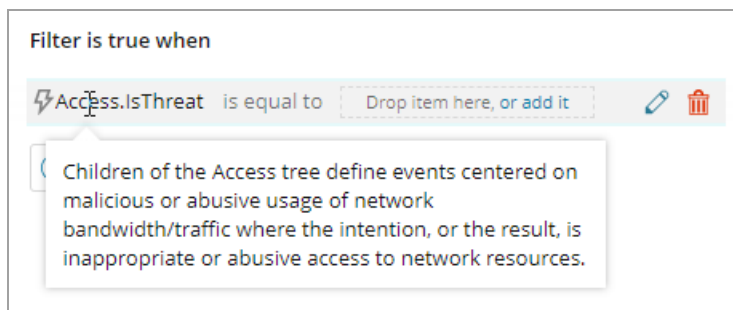
b. Drag the entity or field to the panel.

When an entity is selected and then you select and drag a field, the entity and field are included together.

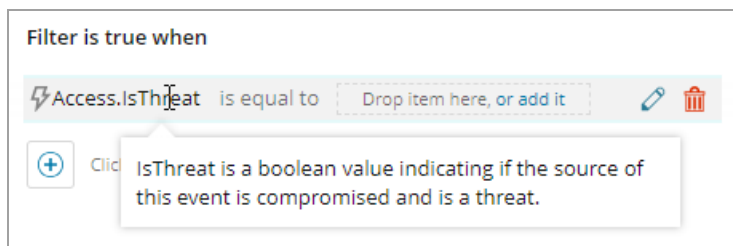
 When you drag a filter field into the filter builder, the place to drop it is illuminated with a blue line.



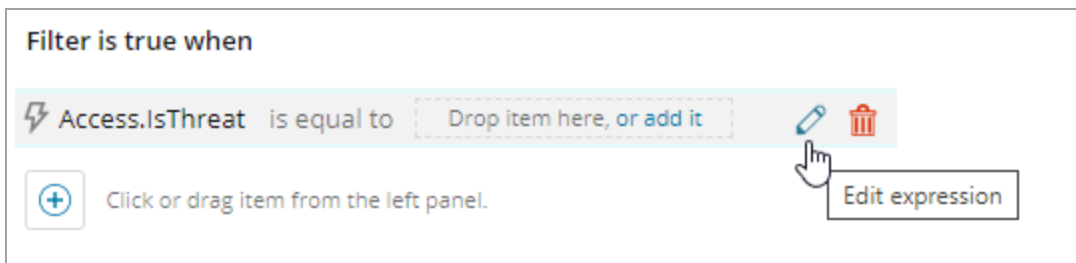
c. Hover your mouse cursor over the filter name to view a description of the entity...



...and the corresponding field.



d. Click the edit  icon.



Filter is true when

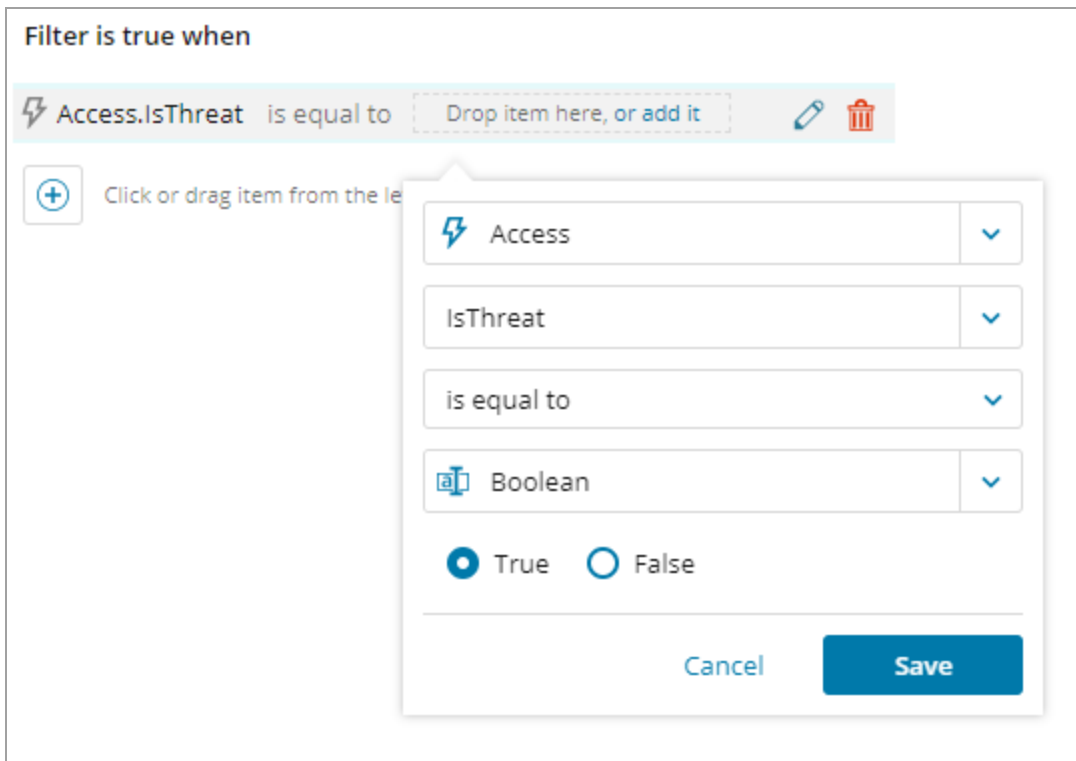
⚡ Access.IsThreat is equal to Drop item here, or add it

+ Click or drag item from the left panel.

Edit expression

- e. Click the drop-down menus to change this to your required condition.

For example, in this case the only meaningful change you can make is from "Access.IsThreat is equal to True" to "Access.IsThreat is equal to False".



Filter is true when

⚡ Access.IsThreat is equal to Drop item here, or add it

+ Click or drag item from the left panel.

Access IsThreat is equal to Boolean

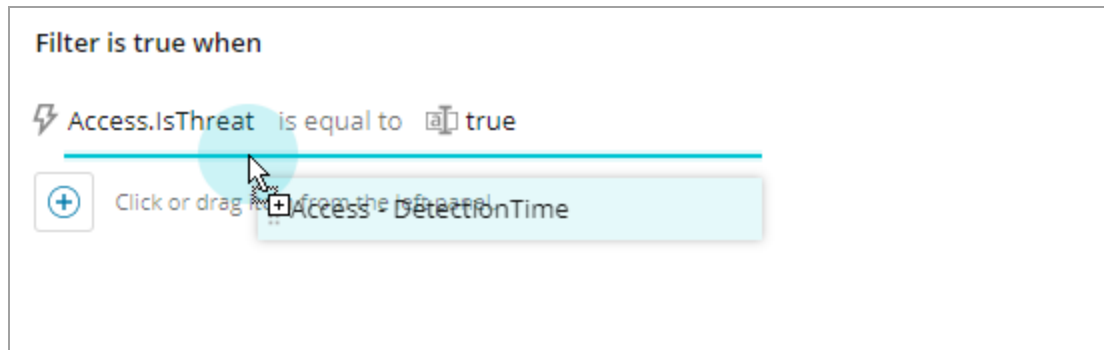
☒ True ☐ False

Cancel Save

Other conditions can involve strings, numerical values, or group values (see below for using group values). For information on using operators (such as "is equal to", "is in", etc) see [Compare values with operators](#).

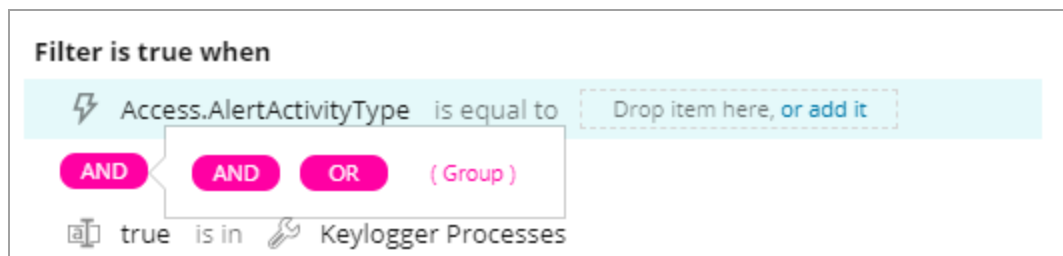
- f. When you are finished, click Save.

7. To add additional conditions, drag the required field beneath the previous condition. A blue line displays where to drop it.

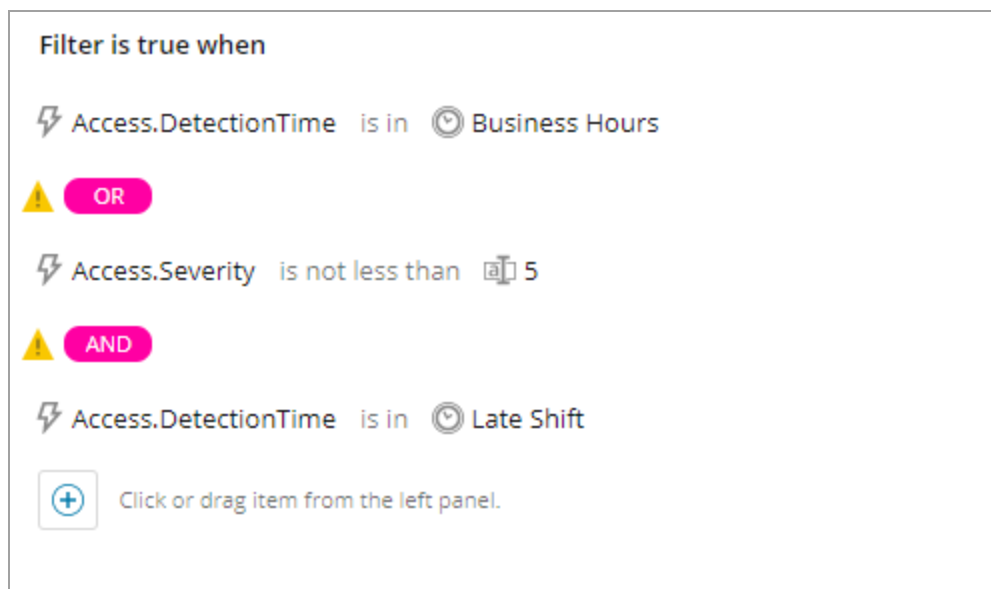


Initially, multiple conditions are assumed to be additive, and the AND operator is displayed.

8. Click AND, and then select OR to change the operator.



If you create a multiple condition that combines conditions with AND and OR operators, group the conditions accordingly. For example, the following condition flags an error as the condition is ambiguous.



9. Click on AND, and select Group.

In the following configuration, the detection time occurs during business hours or events where the detection time occurs during the late shift.

Filter is true when

⚡ Access.DetectionTime is in ⌚ Business Hours

⚠ OR

⚡ Access.Severity is not less than 📏 5

⚠ AND

AND OR (Group)

⚡ Access.DetectionTime is in ⌚ Late Shift

+ Click or drag item from the left panel.

The condition is redisplayed.

Filter is true when

⚡ Access.DetectionTime is in ⌚ Business Hours

OR

(

⚡ Access.Severity is not less than 📏 5

AND

⚡ Access.DetectionTime is in ⌚ Late Shift

)

+ Click or drag item from the left panel.

10. Click Save to save the filter. The filter is now available in the left column.

Compare values with operators

This section covers the use of operators when creating filters in SEM.

Operators in a single condition

When creating operators in a single condition, use the following guidelines:

- When comparing two numeric values, the full range of mathematical operator options is available.
- An IP address is treated as a string (or text) value. Therefore, operators are limited to equal and not equal.
- DateTime fields have a default value of > Time Now, which means, greater than the current date and time.

The following table describes each operator and how it should be interpreted when used as a filter condition.

 A list item (indicated with an * in the following table) can be another event variable, such as an event field. For example, to evaluate if an event's source is equal to a certain destination, compare two event fields, such as `SourceMachine = DestinationMachine`.

Operator	Description
Exists	Use these operators to specify if a particular event or Event Group exists. Read conditions with these operators as follows: This [event/Event Group] must [exist/not exist].
Not exist	
is in	Use these operators when comparing event fields with groups (such as Event Groups, User-Defined Groups, etc.). They determine the filter's behavior, based on whether or the field is contained a specific Group.
is not in	Read conditions with these operators as follows: • This [event field] must be in this [Group]. • This [event field] must not be in this [Group].
Equals	Read conditions with these operators as follows: • This [event variable] must equal this [list item*]. • This [event variable] must not equal this [list item*].
Does not equal	
	Text comparisons (for IP addresses, host names, etc.) are limited to equal or not equal operators.

Operator	Description
Greater than	Read conditions with these operators as follows: - This [event variable] must be greater than this [list item*]. - This [event variable] must be greater than or equal to this [list item*]. - This [event variable] must be less than this [list item*]. - This [event variable] must be less than or equal to this [list item*].
Greater than OR equal to	
Less than	
Less than OR equal to	
AND	Conditions and groups of conditions are subject to AND and OR comparisons. - The AND symbol means two or more conditions (or groups) must occur together for the filter to apply. This is the default comparison for new groups. - The OR symbol means any one of several conditions (or groups) may occur for the filter to apply. When comparing groups of distinct events, you must use the OR symbol.
OR	If you click an AND operator, it changes to an OR, and vice versa.

AND and OR Operators linking multiple conditions in a filter

Filter groups and conditions, and rule groups and correlations, are all subject to AND and OR conditions. By default, new groups, conditions, and correlations appear with an AND condition. Both AND and OR conditions can surround nested groups, and they can be used between groups on the same level to create complex filter conditions or rule correlations.

Example	Description
If x AND y AND z occur, report the event.	If all the conditions apply, report the event.
If x OR y OR z occurs, report the event.	If any of the conditions apply, report the event.
If (x AND y) OR z occurs, report the event.	If conditions x and y occur, or if condition z occurs, report the event.

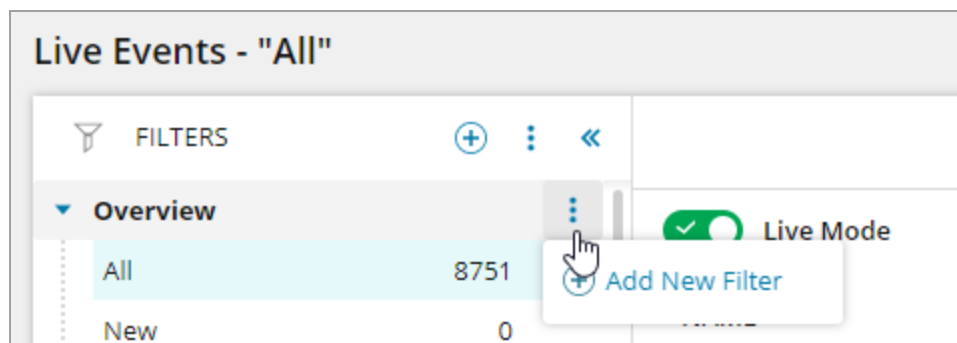
Example	Description
If (a AND b) OR (x AND y) OR (z), occurs, report the event.	In this case, you would create three groups, two nested within the third: • The nested groups are configured as (a AND b) and (x AND y), joined with an OR. • The outer group is configured as (z), surrounding the nested groups with an OR.
Condition1 AND Condition2 AND Condition3 OR Condition4 AND Condition5.	In this example, the filter reports the event when it meets the following conditions: Condition1 and Condition2 and Condition3, or Condition1 and Condition4 and Condition5.

Example filter: View network traffic from specific computers

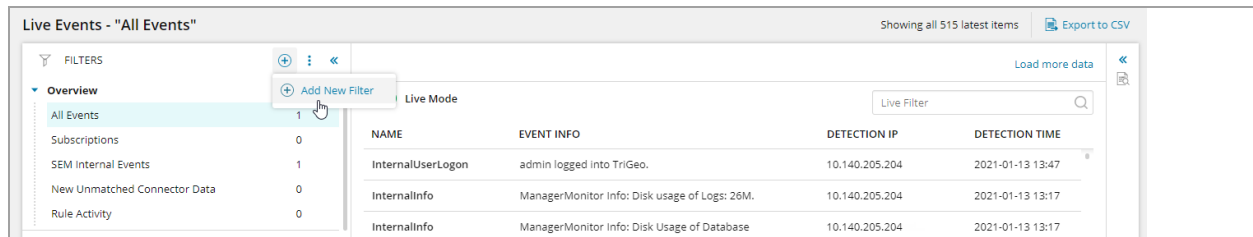
You can create custom filters to highlight specific firewall events. For example, to monitor traffic from a specific computer, create a filter for all network traffic coming from the targeted computer. Use connector profiles and other groups to broaden or refine the scope of custom filters.

The following procedure provides an example of a filter that monitors all traffic from a targeted computer.

1. Log in to the SEM Console.
2. On the toolbar, click Live Events.
3. To create a filter at a group level in the Filters pane, move the mouse pointer over a group heading to expose the vertical ellipsis, and select Add New Filter. For example, to add a filter to the Overview group, click the vertical ellipsis after Overview, and click Add New Filter.



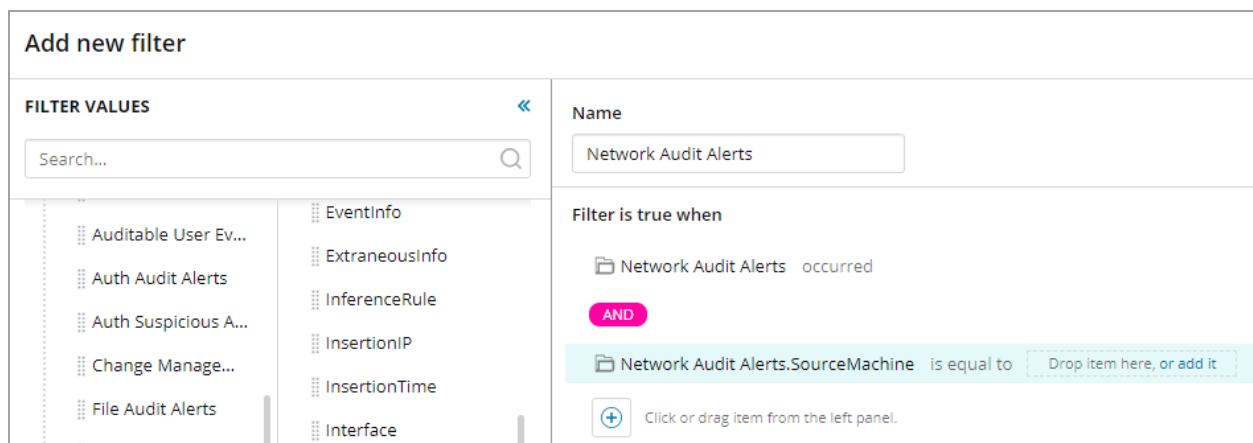
To create a filter at the root level outside of all the groups, click the add  icon, and select Add New Filter.



- In the Name field, enter a descriptive name for your new filter.
- In the first column of the Filter Values, expand Event Groups and drag Network Audit Alerts into the filter builder.

When you drag a value into the filter builder, the correct drop location is illuminated with a blue line.

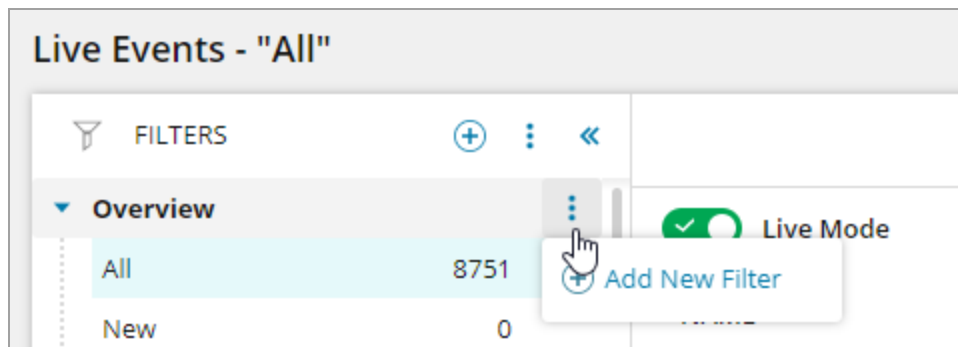
- From the second column of the Filter Values, drag SourceMachine to the filter builder



- Mouse over Network Audit Alerts.SourceMachine to expose the filter builder toolbar.
- Click the "or add it" link and enter the fully qualified domain name of the computer.
- Click Save.

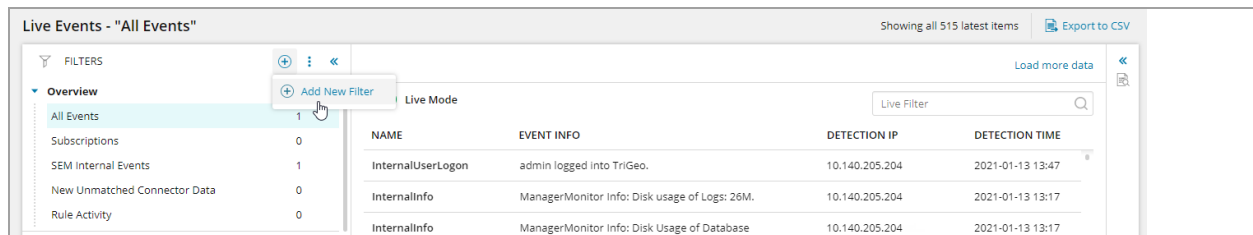
Example filter: Create a filter for all activity in a connector profile

- Log in to the SEM Console.
- On the toolbar, click Live Events.
- To create a filter at a group level in the Filter Values pane, for example, the Overview group, move the mouse pointer over a group heading to expose the vertical ellipsis, and click Add New Filter.



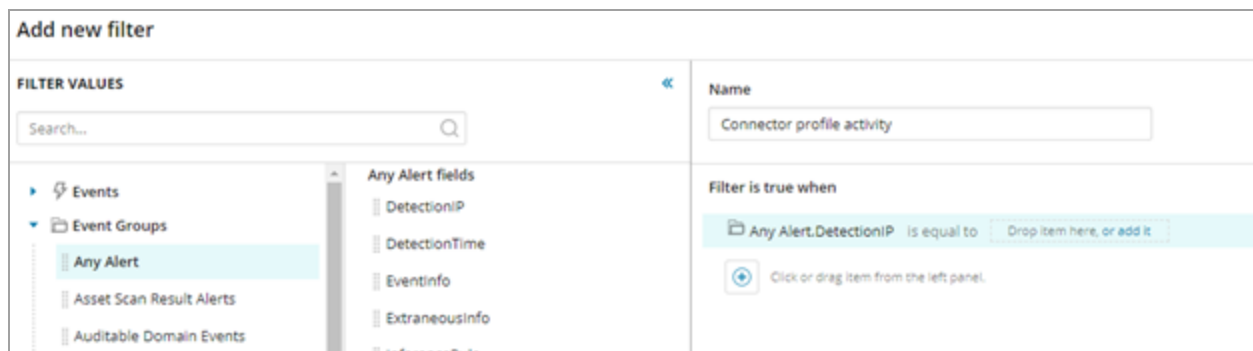
Or:

To create a filter at the root level, click the add  icon, and then select Add New Filter.

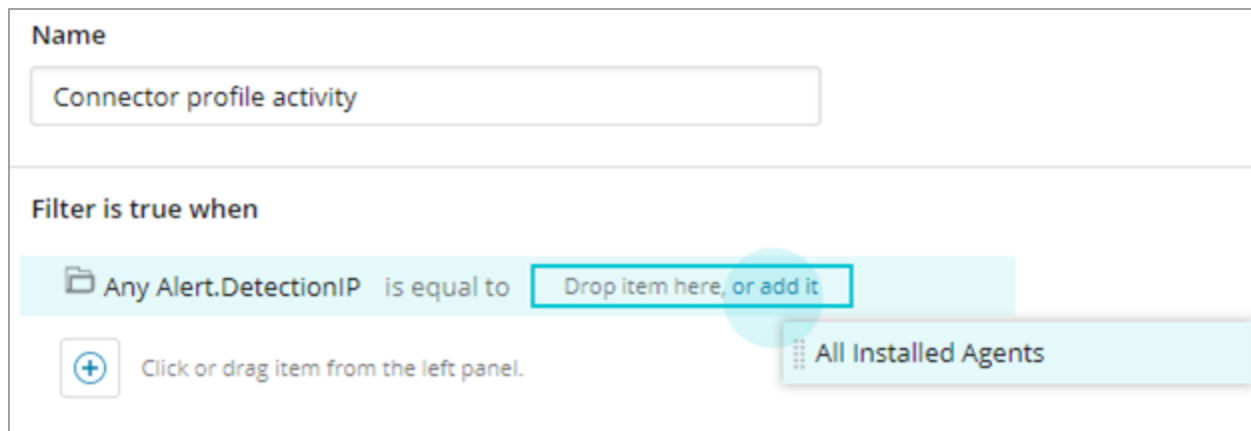


4. Enter a descriptive name for your new filter in the Name field on the right.
5. In the first column under Filter Values on the left, expand Event Groups, and select Any Alert.
6. Drag DetectionIP from the second column on the left into the filter builder.

When you drag a value into the filter builder, the correct drop location is illuminated with a blue line.



7. In the same way, expand the Connector Profiles group, select your profile, and drag it into the filter value drop location.



8. Click Save.

Capture traffic from a specific device

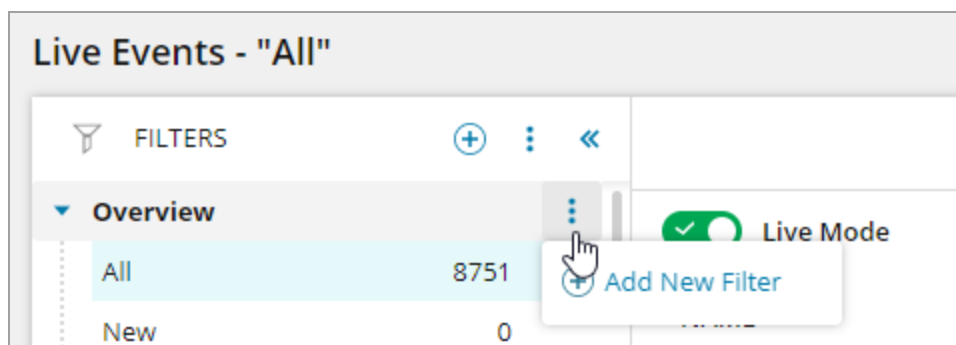
Use the ToolAlias field in SEM rules and filters to capture traffic from a specific device.

The ToolAlias field allows you to create filters, rules, and searches that target traffic from a specific device. Every device that sends events to SEM includes an Alias property you can customize with a device-specific name. Use the ToolAlias field to examine the Alias property and find events that match your filter criteria.

You can also use the DetectionIP event to monitor events from a device that has a specific IP address, for example AnyAlert.DetectionIP=10.1.1.1.

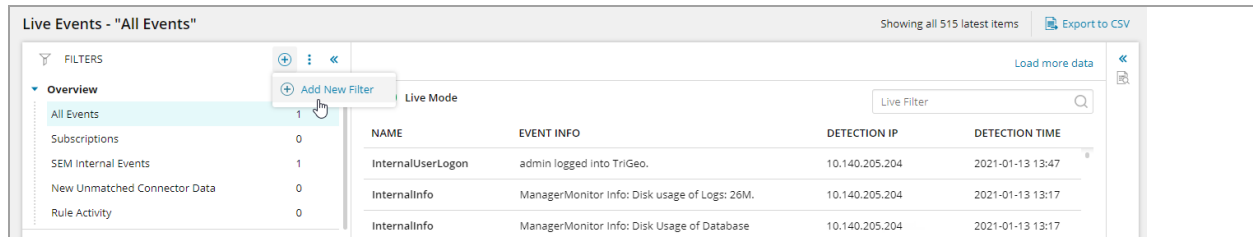
Create a filter to capture events from a specific device

1. On the SEM Console, click the Live Events tab.
2. To create a filter at the group level in the Filter Values pane, move the mouse pointer over a group heading to expose the vertical ellipsis, and then select Add New Filter.



Or:

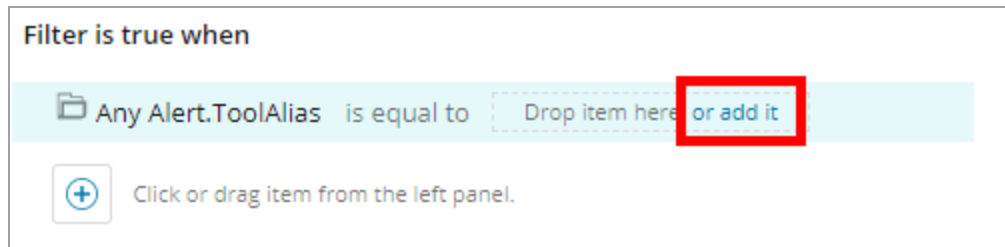
To create a filter at the root level, click the add  icon, and then select Add New Filter.



3. Enter a descriptive name for your new filter.
4. In the first column on the left, expand Event Groups and select one of the following:
 - To view all traffic from your device, select Any Alert.
 - To view all network events from your device, select Network Audit Alerts.
 - To view web traffic from your device, select WebTrafficAudit from the Event groups.
5. From the second column list, drag ToolAlias into the filter builder.

When you drag a value into the filter builder, the correct drop location is illuminated with a blue line.

6. Click the **or add it** hyperlink.



7. Enter a filter value to match the alias property of the device that you want to track. Use asterisks (*) as wildcard characters if required.

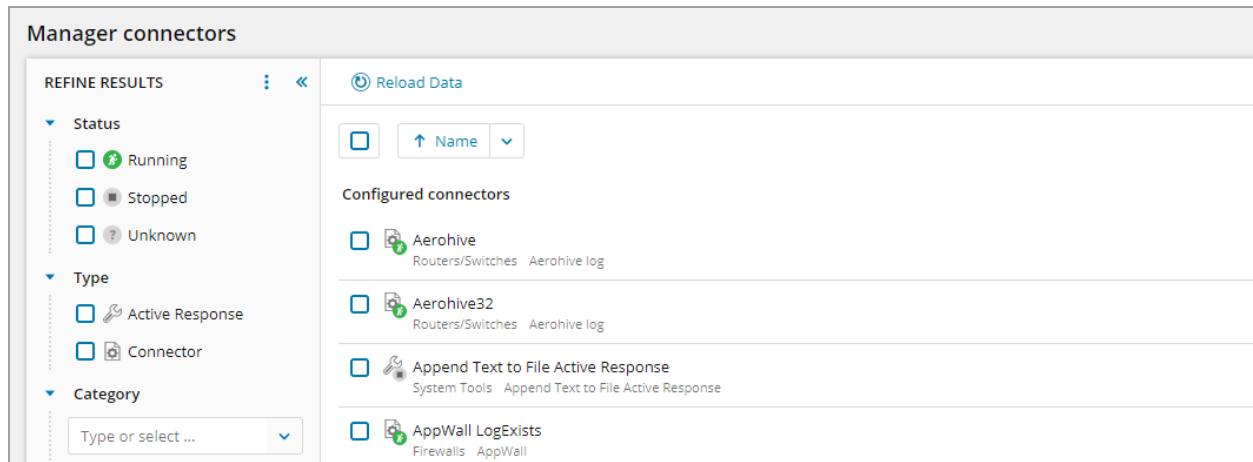
For example, consider the default Firewall filter. Its condition is `Any Alert.ToolAlias = *firewall*`. This assumes that the firewall connector was configured with a Tool Alias that includes "firewall" in the name.

8. Click Save.

Verify that the correct Alias value is associated with the connector

The following procedure applies to devices configured to send logs to SEM. To verify agent connectors, use this same procedure, but apply it to the agent associated with the connector instead.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Manager connectors.
3. Under Configured connectors, select the connector instance you want to verify.



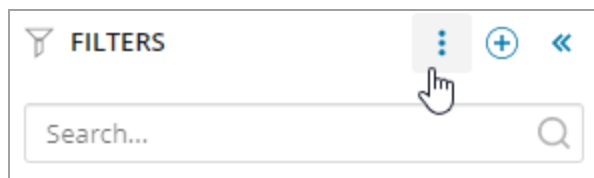
4. On the connector toolbar, click Edit.
5. Verify the connector name (alias) is correct (change the name, if not), and click Save.
6. On the connector toolbar, click Start.

Export and import live event filters in SEM

You can export and import live event filters from SEM as a single file in JSON format.

Export all filters

1. Log in to the SEM Console.
2. On the toolbar, click Live Events.
3. In the Filters column, click the ellipsis  and select Select All Filters.



 You cannot export single or selected filters.

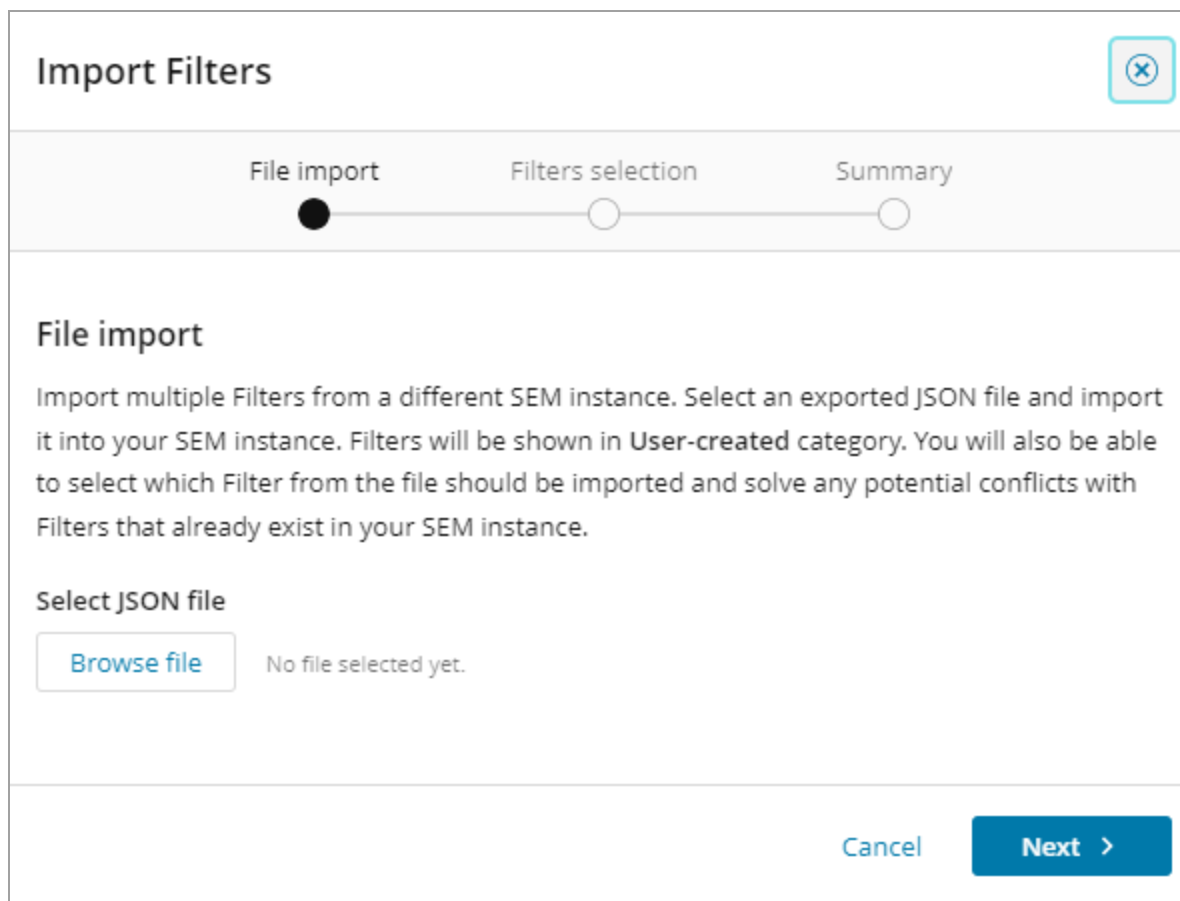
4. Enter a filename, and then click Save.

Import filters

1. Log in to the SEM Console.
2. On the toolbar, click Live Events.
3. In the Filters column, click the ellipsis  and select Import filters.



The Import Filters window is displayed.



4. Click Browse file, navigate to the required JSON file, and click Open.
5. Click Next.

The filters contained in the selected JSON file are listed.

Import Filters ✕

File importFilters selectionSummary

⚠ Invalid filters. 7 of 207 filters are invalid. These filters cannot be imported

☒

↑ Name ↓

Search...

🔍

☒ fsd rew

☒

☒ <img src="sdfs"&am...

☒ ../../../../etc/passwd

☒ 112

☒ 1122

☒ 2

Cancel

< Back

Next >

6. Deselect the filters you do not want to import, and then click Next.

7. Deselect the filters you do not want to import, and then click Next.

The import process begins. The filters that are imported or not imported are indicated in the window.

The dialog box is titled "Import Filters" and has a close button (X) in the top right corner. It features a progress bar with three steps: "File import" (checked), "Filters selection" (checked), and "Summary" (active). The "Summary" section shows two items: "Not imported" (fsd rew) with a red exclamation mark icon and a "Name conflict" error message, and "Imported successfully" (New tool data) with a green checkmark icon. An "Ok" button is located at the bottom right.

8. When the import is complete, click OK.

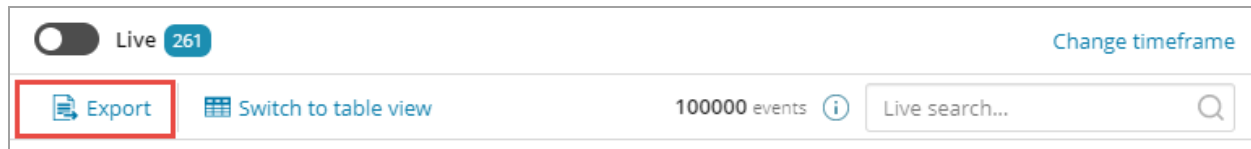
Filter and export event logs

You can filter and export your event logs to a CSV file from the SEM Console. Use CSV files to attach search results to a help ticket, share with members of your team, archive data for historical reference, and more. Each exported record includes the date, time, severity level, IP address, node, source, and message.

1. Log in to the SEM Console.
2. On the toolbar, click Live Events.
3. Set your search parameters, and then initiate your search. The number of returned events appears above the Live Mode toggle button.

 You can export records from live mode, paused mode, and historical search. The number of returned historical events is determined by your [search results threshold](#) on the Settings page.

4. Click Export.



5. Change the location and name of the download file if necessary. and click Save.

By default, the file will be named:

yyyy_mm_dd_hhmm.csv

SEM exports the CSV file to your local system.

Analyze historical data

The [Historical Events and Report screen](#) allows you to locate all event data that passed through a particular SEM Manager instance. Use this screen to perform custom searches, investigate your search results and event data, and identify trends in your network.

You can use the Historical Events screen to:

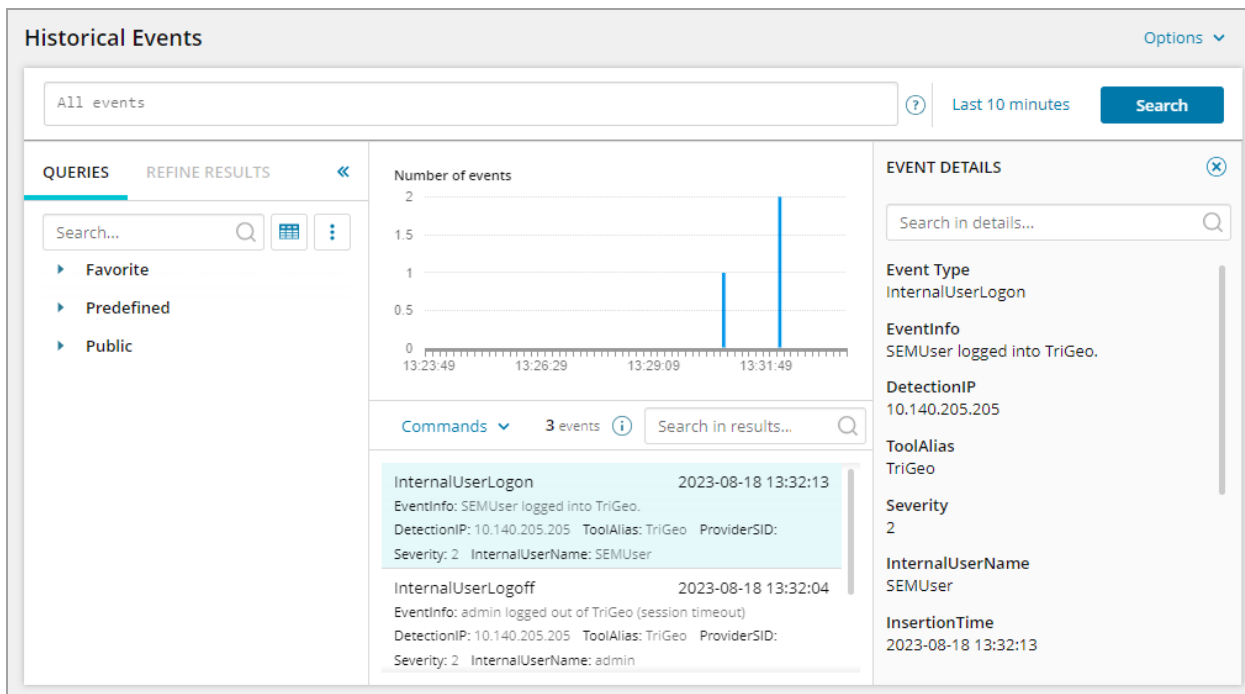
- [Create, save, and schedule](#) a search query
- [Generate a query report](#)
- [Manage and load saved search queries](#)
- Apply query tags and thresholds
- [Export historical search results](#)
- [Import and export historical event queries](#)

 Because some search parameters can result in several matching results and negatively impact SEM performance, SEM limits the number of events that are retrieved. See [Event Limits](#) for more information.

Historical Events and Reports screen

Log in to the SEM console and click Historical Events & Reports in the toolbar. This screen displays the unfiltered events for a specific period of time (such as the last 10 minutes) in graphical and list format.

The following example displays the results for a selected event (highlighted in blue).



This screen includes the following features:

- [Query Builder](#)
- [Time Picker](#)
- [Query options](#)
- [Queries and Refine Results tabs](#)
- [Events chart](#)
- [Events count](#)
- [Events details](#)

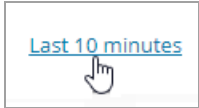
Query Builder

The Query Builder helps you create queries to filter the normalized historical events. Enter a query in the field and then click Search to run the query. See [Create a search query](#) for information about creating queries.

After you create a query, you can [apply tags to queries](#) so they can be grouped for use with the Scheduled Query Severity and Scheduled Query Table Severity widgets on the [SEM dashboard](#).

Time Picker

The Time Picker allows you to [select a time period](#) for the query. Click the time period link (for example, Last 10 minutes) to display results for your selected time period. You can use preset "quick picks" or create your own custom periods.

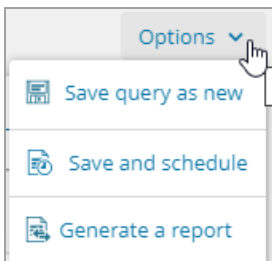


When you click the link in the toolbar, you can refine your search results with the custom time picker. You can select a quick pick, or set a specific date and time range.

QUICK PICKS	CUSTOM RANGE
Last 10 minutes	Start
Last 30 minutes	09 Aug 2023 
Last 1 hour	10:19 AM 
Last 2 hours	End
Today	09 Aug 2023 
Last 24 hours	10:29 AM 
Last 7 days	
Last 30 days	

Query options

After you create a query, click Options in the toolbar to save the query, save and schedule the query, or generate a query report.



The following table describes the query options.

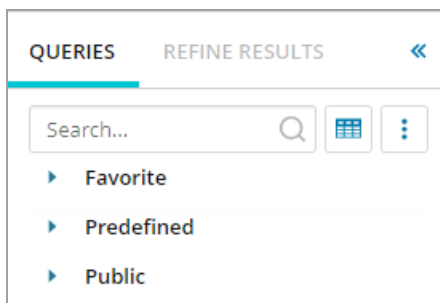
Selection	Definition
Save query as new	Saves the current query with a user-supplied name. When you are finished, the query will be available from the Queries tab in the Public drop-down menu. After you save a new query, click Options in the toolbar and select Edit saved query in the drop-down menu. When you edit a query, you can change the query name, add a tag, and modify the thresholds used to determine the severity level and colors on the Dashboard overview widgets.
Save and schedule	Runs the currently viewed query at specified dates and times. When you click this option, you can provide a name for the query and schedule the query search. You can have the results emailed to selected email addresses and LDAP users or used in Scheduled Query Severity dashboard widgets. See Schedule a search query for details on how to schedule a search query.
Generate a report	Generates a query report. See Generate a query report for details on how to generate a report.

Queries and Refine Results tabs

The Queries and Refined Results tabs in the left column allow you to switch between your list of saved historical event queries and refined results.

Queries tab

The Queries tab in the left column lists your saved historical event queries. All historical event queries are divided into four categories: Favorite, Predefined, Public and User-created, as shown below.

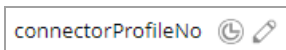


The following table describes the Queries tab categories. See [Create a search query](#) for details about creating queries.

Category	Description
Favorite	Lists queries that were created in other categories but marked by you as favorites.
Predefined	Lists the most commonly required queries.
Public	Lists queries that can be used by any SEM user in your deployment
User-created	Lists all queries created by you for your own use and are not accessible or editable by other users.  This category displays in the Queries tab after you create and save a query. By default, all queries you create are only visible and used by you. However, you can share queries and make them editable. See Manage and load saved search queries for details about managing search queries.

Query icons

Some saved historical event queries include icons that provide addition information about the query. For example:



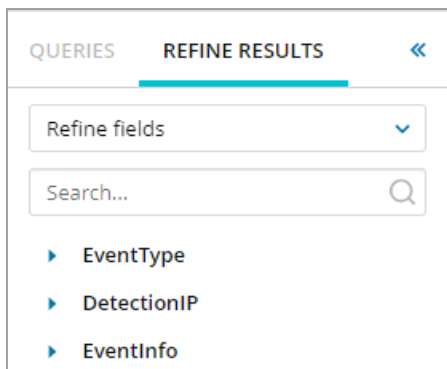
The following table describes each icon that provides additional information about the saved query.

Tag	Description
	The saved query is scheduled to run at a specific date and time. The user who created this query can configure the query to automatically send the query results to a selected email address or LDAP user or display the results in the Scheduled Query Severity dashboard widget.  The scheduled query widgets are created and customized in the same way as other SEM Dashboard widgets.
	The saved query was created by the current user and shared with everyone. Only the current user can edit the query.

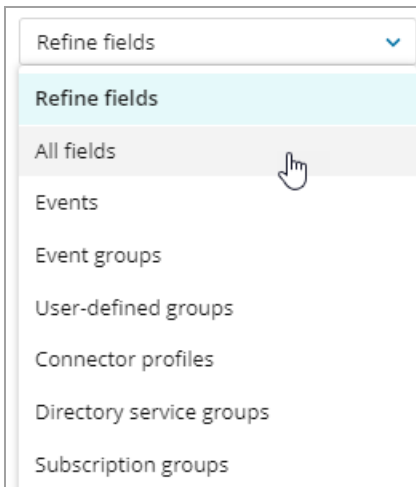
Tag	Description
	The shared query is read-only and cannot be modified by the current user. The user who shared the query can stop sharing the query at any time. You can copy the shared query. The copied query is moved to the User Defined category where you can rename and edit the query.
	The saved query can be edited by anyone. After a query is configured as editable, it cannot be made non-editable or private.
	The saved query is a favorite and saved in your Favorite drop-down menu. To copy a query to the Favorite query menu, select the query, click the vertical ellipsis, and select Favorite. To remove a query from the Favorite query menu, select Remove from favorites.

Refine Results tab

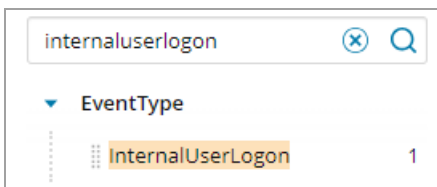
The Refine Results tab in the left column lists the fields available for filtering historical events by category. You can drag these fields into the Query Builder field when you [create a search query](#).



To organize the results by all fields, events, connector profiles, or specific groups, click the drop-down menu and select an option.

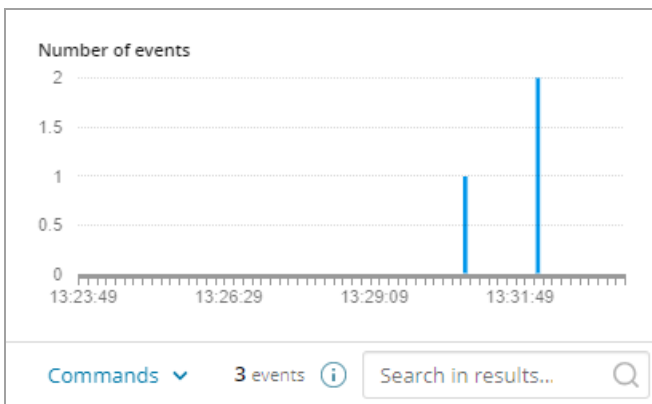


To locate and a historical event, enter an event in the Search box and then click the magnifying glass icon  to display the result.

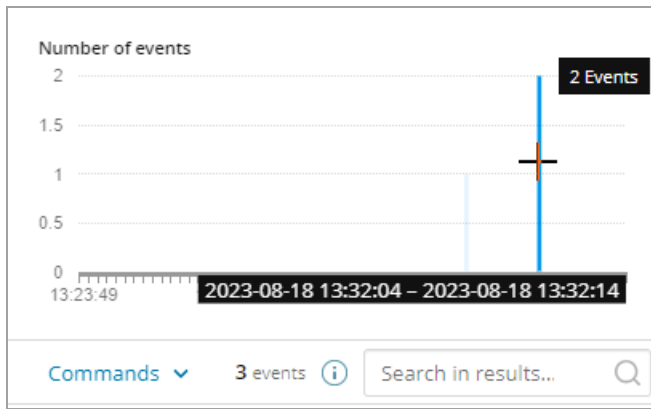


Events chart

The event chart displays the number of events over the specified period of time as a simple bar chart.



Drag the cursor over a time period to zoom in on that period.



In the toolbar, the Commands drop-down menu provides the following options:

- Click [Export](#) to save the filtered events as a CSV file.
- Click Switch to List view to display the filtered events as a list.
- Click Switch to Table view to display the filtered events as a table.
- Click Hide Chart to remove the chart from display.
- Click Show Chart to display the chart.

The toolbar also displays the [maximum number of events](#) that meet your query, and allows you to search the event results for a specific event.

Events count

The toolbar also displays the maximum number of events that meet your query, and allows you to search the event results for a specific event.



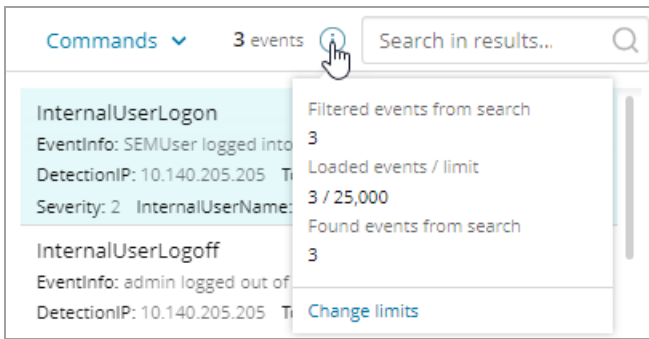
Click the  icon to view the following:

- Number of loaded events
- Maximum number of loaded events
- Number of event found (loaded and not loaded)

Because searches with a high maximum threshold can negatively impact performance, you can set the maximum number of loaded events.

On average, every 1000 returned search results consumes approximately 100 MB of RAM. This can result in up to 10 GB consumed by one search query if the threshold is set to 100,000 maximum results.

Click the information icon to display additional information.

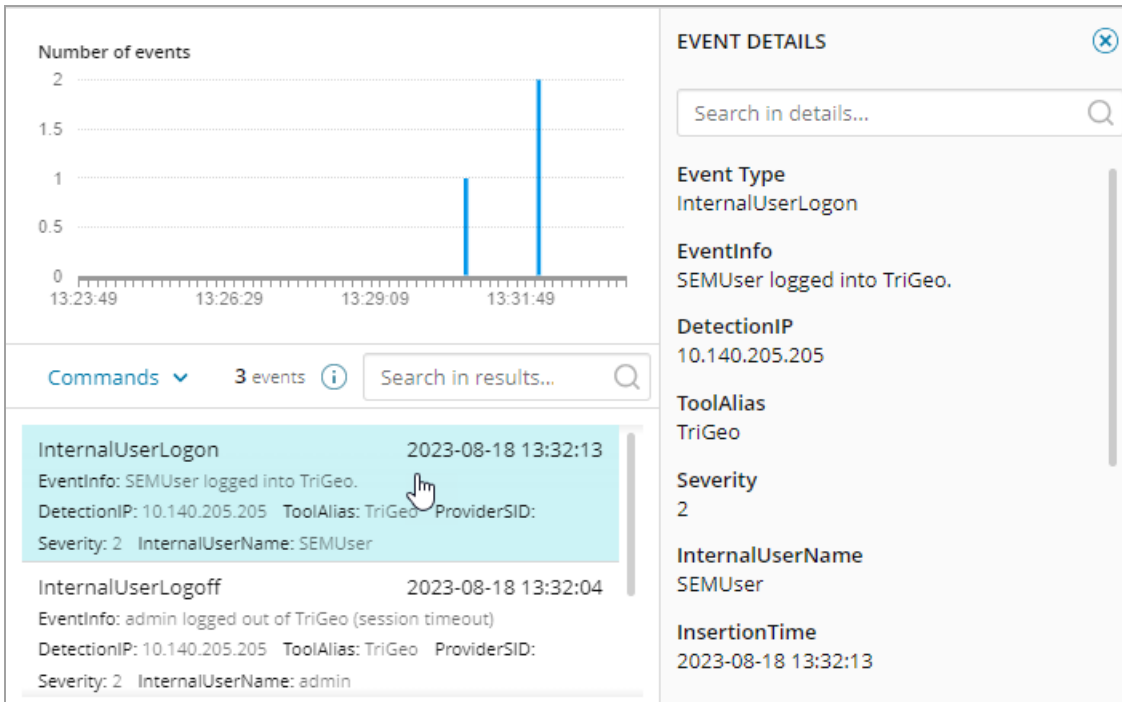


The screenshot shows the 'Commands' dropdown menu open, displaying '3 events'. A search filter dropdown is also open, showing 'Filtered events from search' with '3' results. The search filter dropdown includes a 'Change limits' link.

To change the maximum limit, click Change limits. See [Set live and historical event limits](#) for more information.

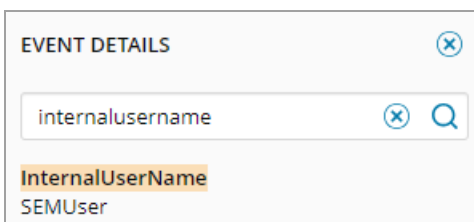
Events details

The Event Details column displays additional information about an event. When you select a single event in the center column, the Event Details column lists the details about the event.



The screenshot shows the 'Event Details' column on the right side of the interface. The 'Event Type' is 'InternalUserLogon'. The 'EventInfo' is 'SEMSUser logged into TriGeo.'. The 'DetectionIP' is '10.140.205.205'. The 'ToolAlias' is 'TriGeo'. The 'Severity' is '2'. The 'InternalUserName' is 'SEMSUser'. The 'InsertionTime' is '2023-08-18 13:32:13'.

To locate specific details in the event, enter a search term in the search field and then click the magnifying glass icon  to view the results.



The screenshot shows the 'Event Details' search results. The search term 'internalusername' is entered in the search field. The results show 'InternalUserName' with the value 'SEMSUser'.

Create a search query

Use the intuitive search builder to create custom search queries. To perform custom searches, click Historical Events in the toolbar.

By default, the initial search period covers the last hour. The search period begins when you go to Historical Events, and stops one hour before.

The following table lists the available operators and functions.

Operator	Definition
=	Equals
!=	Not equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
in	True if the operand is equal to one of a list of expressions.
not in	Displays a record if the condition is not true.
Function	Definition
And	Displays results if all the conditions separated by And are true.
Or	Displays results if all the conditions separated by Or are true.
()	Parentheses: gives solving priority to the conditions inside of the first grouping when more than one grouping is listed.

You can build a query using the following methods:

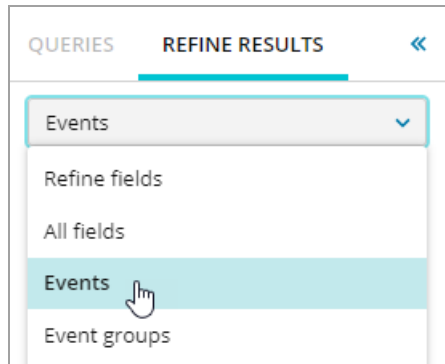
- [Refining the query results](#)
- [Entering the query data](#)

Refine the query results

1. Log in to the SEM Console.
2. In the toolbar, click Historical Events and Reports.
3. In the left column, click Refine Results to list the categories of available fields.

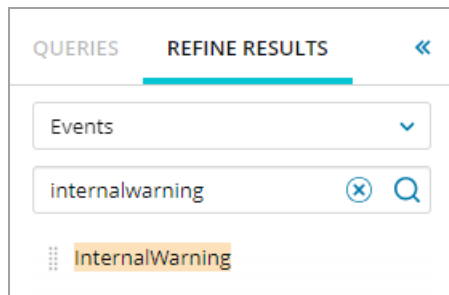
- Click the drop-down menu and select a category.

For example, Events.



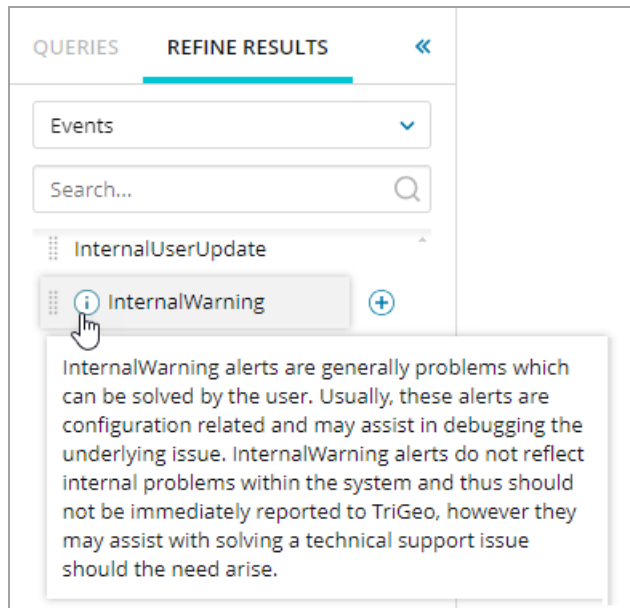
You can also enter a term in the Search field to locate an entity. All matches are highlighted in the results.

For example, InternalWarning.



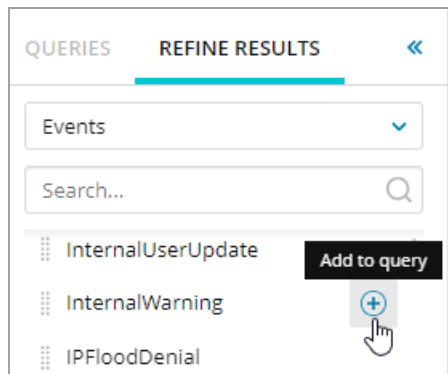
- Select an event entity. Hover over the information  icon to display a description.

For example, click the Events drop-down menu and select InternalWarning.



 All entities listed in the Events menu include context help.

6. Hover over the selected entity and click + to add the query.

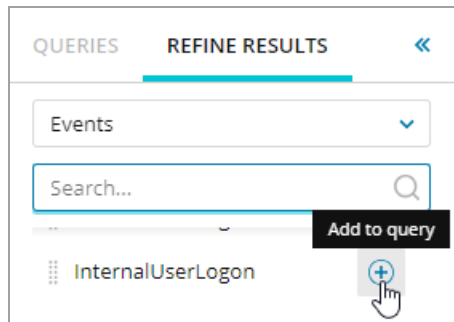


Your selection is added to the query builder.

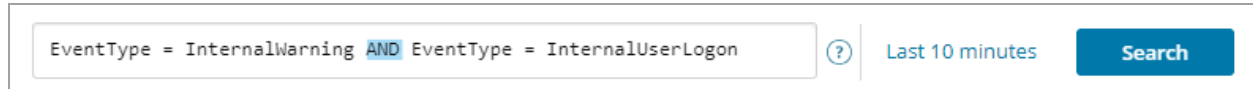


7. Select one or more additional options.

For example:

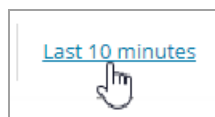


By default, the query is built using AND conditions.

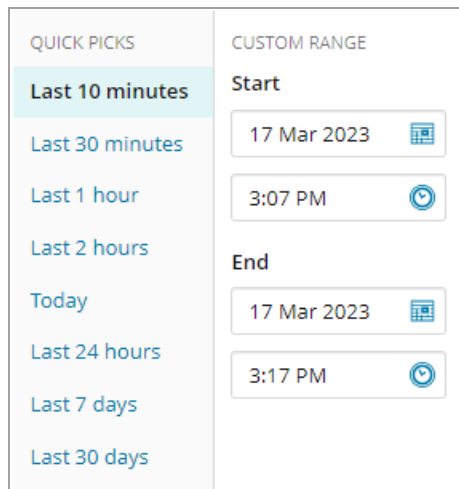


The condition can be changed to an OR condition and parenthesis added as required.

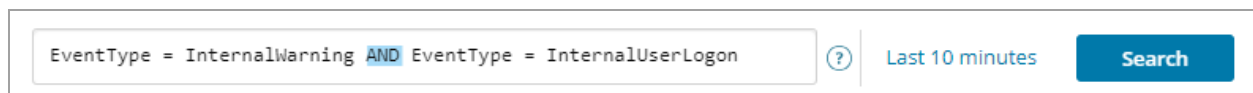
8. Continue adding other fields until you have created your query.
9. Click the time picker (for example, Last 10 minutes).



10. Refine your results using the custom time picker. You can select a quick pick or a specific date and time range.



For example, if you click Last 10 minutes, that value displays next to the query builder.



11. Click Search.

Your results display in the window.

	2024-03-11 14:19:29
Description: Failed to read Office365 audit logs: Oauth...	
EventInfo: Failed to read Office365 audit logs: OauthTo...	
DetectionIP: 10.140.205.205 ToolAlias: semo265test.onmicrosoft.com	
	2024-03-11 14:18:58
Description: Failed to read Office365 audit logs: Oauth...	
EventInfo: Failed to read Office365 audit logs: OauthTo...	
DetectionIP: 10.140.205.205 ToolAlias: semo265test.onmicrosoft.com	
	2024-03-11 14:18:28
Description: Failed to read Office365 audit logs: Oauth...	
EventInfo: Failed to read Office365 audit logs: OauthTo...	
DetectionIP: 10.140.205.205 ToolAlias: semo265test.onmicrosoft.com	

Enter the query data

You can also enter query data in the query builder. As you enter the query, tips and suggestions display to guide you as you enter your parameters.

Historical Events

IP

✖ When a condition has only one operand, the operand must be a string.

IPAddress

⚡ IPFloodDenial

⚡ IPFragmentationAccess

⚡ IPFragmentationDenial

⚡ IPSecTrafficAudit

⚡ IPSourceRouteAccess

⚡ IPSpoofAccess

⚡ IPTrafficAudit

⚡ MalformedRIPAccess

Add the time period for the query

When you create the query fields, use the time picker to select the date range you want the query to cover.

QUICK PICKS	CUSTOM RANGE
Last 10 minutes	Start
Last 30 minutes	17 Mar 2023
Last 1 hour	3:07 PM
Last 2 hours	End
Today	17 Mar 2023
Last 24 hours	3:17 PM
Last 7 days	
Last 30 days	

When your query is complete, click Search to initiate the search.

Query building tips and examples

The query builder supports a combination values, operators, and functions.

Basic query structure

A basic query uses full-text values. For example:

```
someText "
```

You can also chain the conditions using logical operators "AND" and "OR." For example:

```
someText " AND "someOtherText" OR "someOtherText2"
```

To ensure that your conditions execute properly, use brackets (parenthesis). For example:

```
someText " AND ( "someOtherText" OR "someOtherText2" )
```

Advanced conditions

Besides the basic conditions, you can add conditions with two operands connected by an operator.

For example, if you want to search for an event NOT containing certain text, create the event as shown below:

```
Text != "someText"
```

You can search for events containing a value in a specific property.

```
DestinationPort = 1234
```

You can specify the event type and condition.

```
Access.DestinationPort = 1234
```

You can split the event into separate conditions.

```
EventType = Access AND DestinationPort = 1234
```

You can enter name of the event group if it contains non-alphanumeric characters.

```
Any Alert".DestinationPort = 1234
```

Special characters and spaces

Queries support a wide range of special characters, including Unicode characters such as ☹️ 🌞 🎵, for example. One primary restriction is using spaces and double quotes in the names of custom groups and other items a user can create. To use them in a query, wrap the value in quotes.

```
Any Alert".DestinationPort = 1234 OR DetectionIP in
UserDefinedGroup."Auditd Watchers Excludes"
```

If the name or value contains a double quote, it must be doubled in the query.

```
Text = "sometext""containing""quotes"
```

This results in searching for the following text:

```
sometext"containing"quotes
```

Wildcards in strings

You can use wildcards in string values, but their placement is important. The following examples use the asterisk (*) wildcard character.

Starting wildcard

Text	What this will match?	What this will NOT match?	Explanation
*sometext"	"xxx sometext" "sometext"	"xxxsometext" "xxx sometext xxx"	A wildcard at the beginning indicates that other "words" can be before the following text. As a result, "*sometext" and "* sometext" are actually equivalent queries.

Ending wildcard

Text	What this will match?	What this will NOT match?	Explanation
sometext*	"sometext" "sometextxxx" "sometextxxx someothertext"	"xxx sometext" "xxxsometext"	A wildcard at the end of the text WITHOUT a space indicates the value can continue with any other parts. Without a starting wildcard, this query would search for values starting with TEXT "sometext".
sometext *	"sometext" "sometext xxx someothertext"	"xxxsometext" "sometextxxx"	A wildcard at the end of the text separated by a space indicates that after the specified "word," any number of other words in the value would match. Without a starting wildcard, this query would search for values starting with the WORD "sometext".

Wildcard in the text

Text	What this will match?	What this will NOT match?	Explanation
some*text	"sometext" "someothertext"	"xxxsometext" "sometextxxx" "xxx sometext xxx" "some text" "some xxx text"	A wildcard in the middle of the word looks for a "word" that can contains alphanumerical characters in a place of the wildcard. Without starting or ending wildcard this query would look for values containing one WORD starting with text "some" and ending with text "text".

Wildcard combinations

Text	What this will match?	What this will NOT match?	Explanation
*some*text *	"sometext"	"xxx some text"	You can combine wildcards to more complex expressions based on the rules above.
	"someOtherText"	"xxx sometextxxx"	
	"xxx sometext"		
	"sometext xxx someothertext"		

Custom groups

The following groups are supported groups used with the "in" operator:

- SubscriptionGroup
- UserDefinedGroup
- DirectoryServiceGroup
- ConnectorProfileGroup

The following group not supported when used with the "in" operator: Unsupported groups:

- TimeGroup

Since groups do not currently restrict unique names across group types, use the prefix to search for a group

Group Type	Prefix
SubscriptionGroup	Subscription
UserDefinedGroup	UserDefinedGroup
DirectoryServiceGroup	DSGroup
ConnectorProfileGroup	Profile

The query would be similar to the following:

```
DetectionIP in UserDefinedGroup.BlockedAddresses
```

If the name contains non-alphanumeric characters, it would be similar to the following:

```
DetectionIP in UserDefinedGroup."Auditd Watchers Excludes"
```

Hint

This feature suggests possible query values. The provided "hints" are based on cursor position in the input. As you type, hints are filtered to provide more specific options.

Limitations and restrictions

Queries are limited to 10,000 characters.

Troubleshooting

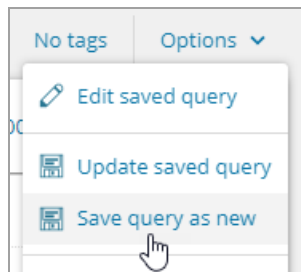
Currently, there is a known issue that hint is horizontally misaligned to the input. In some occasions, the hint suggestions may be vertically misaligned to the input. To fix the issue, close or open it.

Save a search query

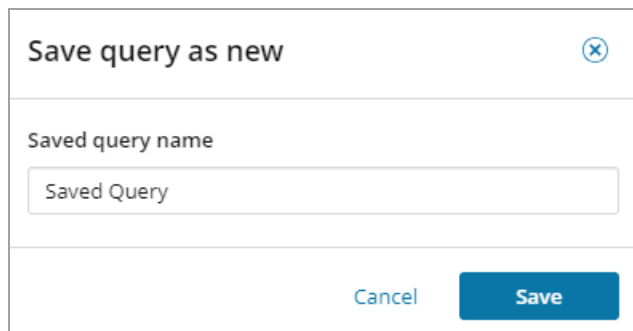
After you create a search query that meets your requirements, save the query for future use.

i If you load a saved query and make changes to it, an additional menu entry is displayed, enabling you to update the saved query.

1. [Create a search query.](#)
2. Click the Options drop-down menu and select Save query as new.

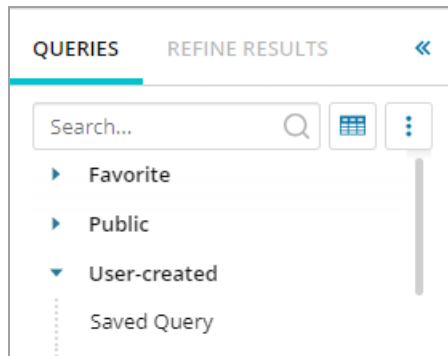


3. Enter a name for the query.

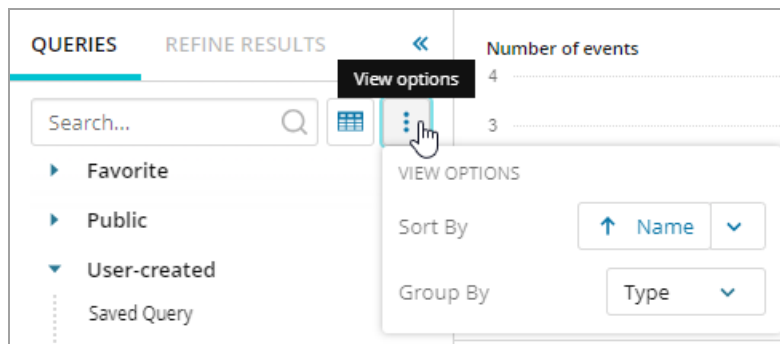

 A screenshot of a dialog box titled 'Save query as new' with a close button (X) in the top right corner. Inside the dialog, there is a label 'Saved query name' above a text input field. The input field contains the text 'Saved Query'. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Save'.

4. Click Save.

The query is saved in the User-created menu.



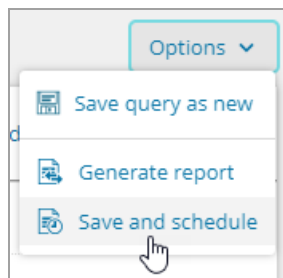
To access the User-created menu, click the vertical ellipsis and select the following Sort By and Group By options:



Schedule a search query

Scheduling a query means it can be run automatically at set times and days, and the results sent to one or more email addresses or used in [dashboard widgets](#).

1. [Create a search query](#).
2. Click the Options drop-down menu and select Save and schedule.



i If you are scheduling a saved query, select Schedule query.

3. Enter a unique name for this query, and then click Save.

Save query as new ✕

Saved query name

My Scheduled Query

Cancel

Save

4. Select when you want the query to run. This can be daily, weekly or monthly.
5. Select the time or times on the selected day or days that you want the query to run.
6. Select the start and optional end date.

7. Enter or select the email addresses to which you want the results of this query to be sent. You can add LDAP users if you have configured SEM for LDAP.

Schedule search - my query

OCCURRENCE

Run search

Daily

every

1

^

v

day

EXECUTION TIME

4:23 PM

+ Add time

EXECUTION PERIOD

Starting on

19 Aug 2020

☐

Ending on

EMAIL

Recipients

Select recipients...

Add LDAP users

Email template: Scheduled Search

Cancel

Schedule

8. Click Schedule.

Generate a query report

You can generate a query report in CSV for PDF format.

1. Log in to the SEM console.
2. Click Historical Events in the toolbar.

- In the left column, click the Queries tab.

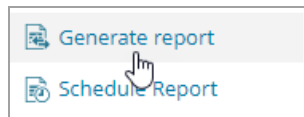


- Maximize a query category and select a query for your report.

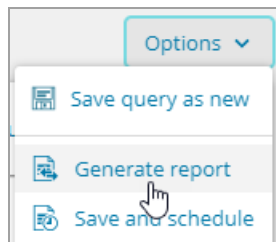


See [Analyze historical data](#) for a description of all query icons.

- Mouse over the query name, click the vertical ellipsis , and select Generate report.



You can also click the Options drop-down menu in the top toolbar and select Generate a report.



- In the Generate Report dialog box, the Name field defaults to the query name. Accept this default name or change the name as required.



A screenshot of the 'Name' field in the Generate Report dialog box. The field contains the text '30 day query'.

- Click the Format drop-down menu and select CSV or PDF as your report format. In the following example, PDF is selected.



A screenshot of the 'Format' drop-down menu. The menu is open, showing 'PDF' as the selected option.

- Click the Group by drop-down menu and select a category used to group the events together. In the following example, all events are grouped together by the event detection IP address.



A screenshot of the 'Group by' drop-down menu. The menu is open, showing 'Detection IP' as the selected option.

9. In the Events Limit field, enter the maximum number of events you want to include in your report. Click the up or down arrows to add or subtract your field value by one event.

The default value is ten million (10000000) events.

Events Limit

^
v

10. Click Generate.

The report is saved to a ZIP file and downloaded to your Windows system.

11. Unzip the file using an unzip utility.
12. Click on the file to view the report data.

The following example provide a partial example of a 30 day query report.

 Due to the size of the report, an additional column of information was excluded from this example.

30 day query					Security Event Manager	
7/8/23 2:13 PM - 8/7/23 2:13 PM, Displaying Events: 100 of 35196					10.140.205.205	
Detection Time	Detection IP	Event Type	Tool Alias	Provider SID	Event Info	
8/7/23 2:12:03 PM	10.140.205.205	InternalAuditSuccess	auditing	report	admin - Report 'superQuery' generated successfully for period: 2023.08.07 20:12:02 CEST to 2023.08.07 21:12:02 CEST	
8/7/23 2:10:50 PM	10.140.205.205	InternalAuditSuccess	auditing	historical-search	admin - Historical search of 21 events has finished	
8/7/23 2:05:38 PM	10.140.205.205	InternalAuditSuccess	auditing	report	admin - Report 'Network Event Data Last Day' generated successfully for period: 2023.08.06 21:05:38 CEST to 2023.08.07 21:05:38 CEST	
8/7/23 2:00:51 PM	10.140.205.205	InternalAuditSuccess	auditing	historical-search	admin - Historical search of 21 events has finished	
8/7/23 1:59:11 PM	10.140.205.205	InternalAuditSuccess	auditing	historical-search	admin - Historical search of 21 events has finished	
8/7/23 1:50:18 PM		FileMove		MoveToDeletedItems	MoveToDeletedItems from folder "Inbox" to "Deleted Items" from . Result: "Success"	

Manage and load saved search queries

Historical event queries can be divided into four categories:

Favorites: Queries that have been created in other categories but marked as favorites appear here. See [Manage search queries](#) for more information.

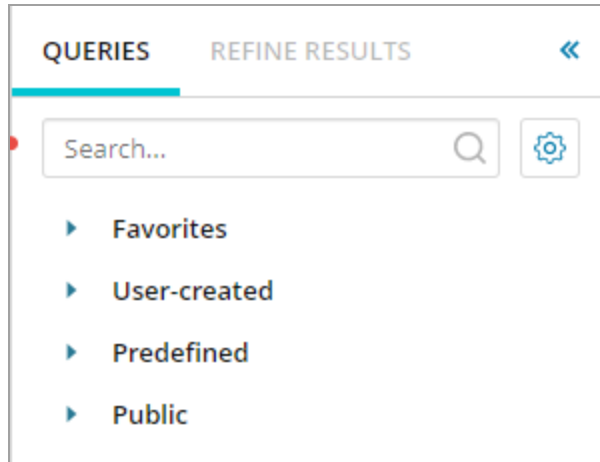
User-created: Queries that have been created by the current user for their own use and have not been made accessible or editable by other users. By default, all queries that you create are only visible to, and usable by, you. However, you can share queries and make them editable, if required. See [Manage search queries](#) for more information.

Predefined: A set of the most commonly required queries set up in advance.

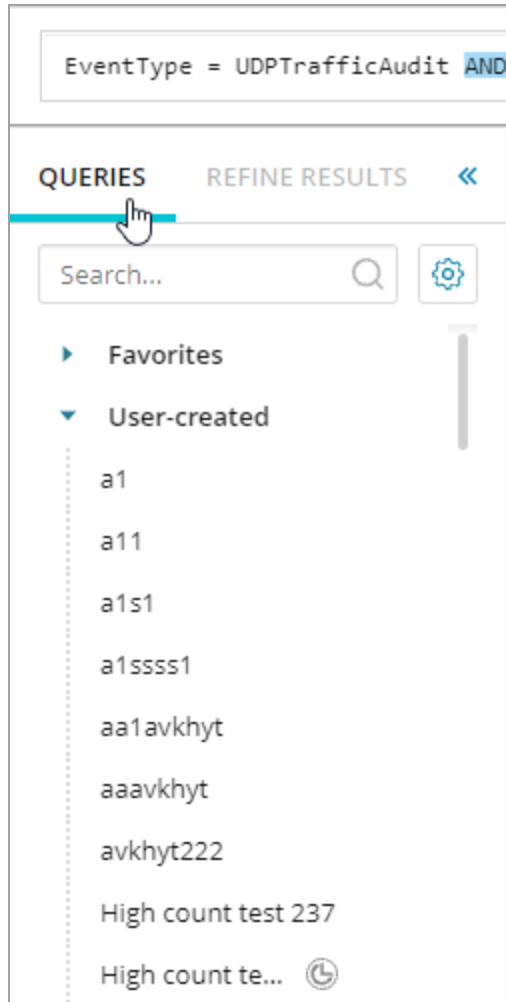
Public: Queries that have been made public can be used by any SEM user on your system. If followed by the Use Only icon  a query can be used but cannot not edited. (However, it can be copied and the copy can be edited.) If followed by the Editable icon , the query can be edited, renamed and saved. Once a query has been made editable, it cannot be made non-editable or made private.

To access queries:

1. Navigate to the Historical Events page.
2. Select the Queries tab in the left column.



3. Click on the required query type.

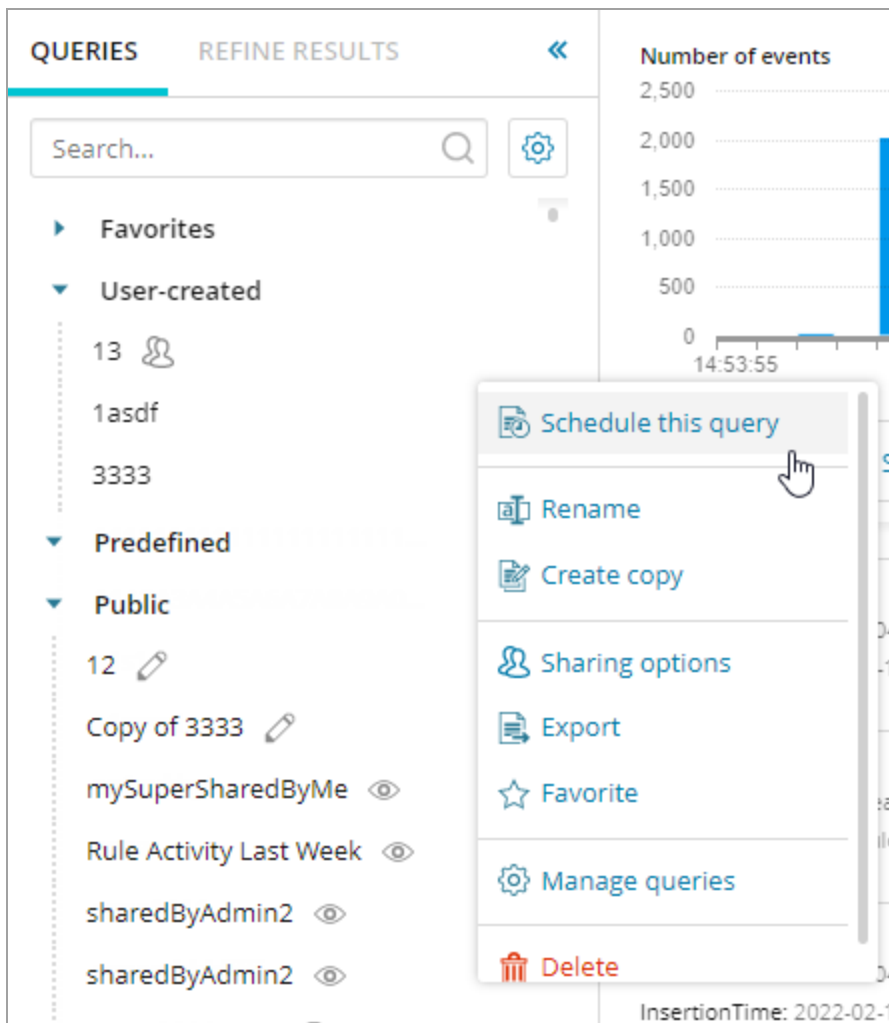


i If a query has a clock icon  after its name then it has a [schedule](#) running.

4. Click a query to load it.

Manage search queries

Search queries can be managed individually by moving the cursor over the query name and clicking the vertical ellipsis icon  that is displayed as shown below:



The available options are mostly self-explanatory:

- Click [Schedule this query](#) to open the [Schedule](#) window for this query. A scheduled query can be unscheduled.
- Click [Rename](#) to change the name of a query. Note you cannot rename a Public query if it has a Use Only icon  by it, and the option is not displayed.
- Click [Create Copy](#) to create an identical copy of a query prefixed with "Copy of". This copy will be placed in the User-Created category.
- Click [Sharing options](#) to make a query public that is usable by other SEM users on your network. You can specify whether you want other SEM users to be able to edit this query (which will be marked with the  icon) or if they are only allowed to use the query exactly as it is (indicated by the  icon.)

Share Query "3333"


Permissions options

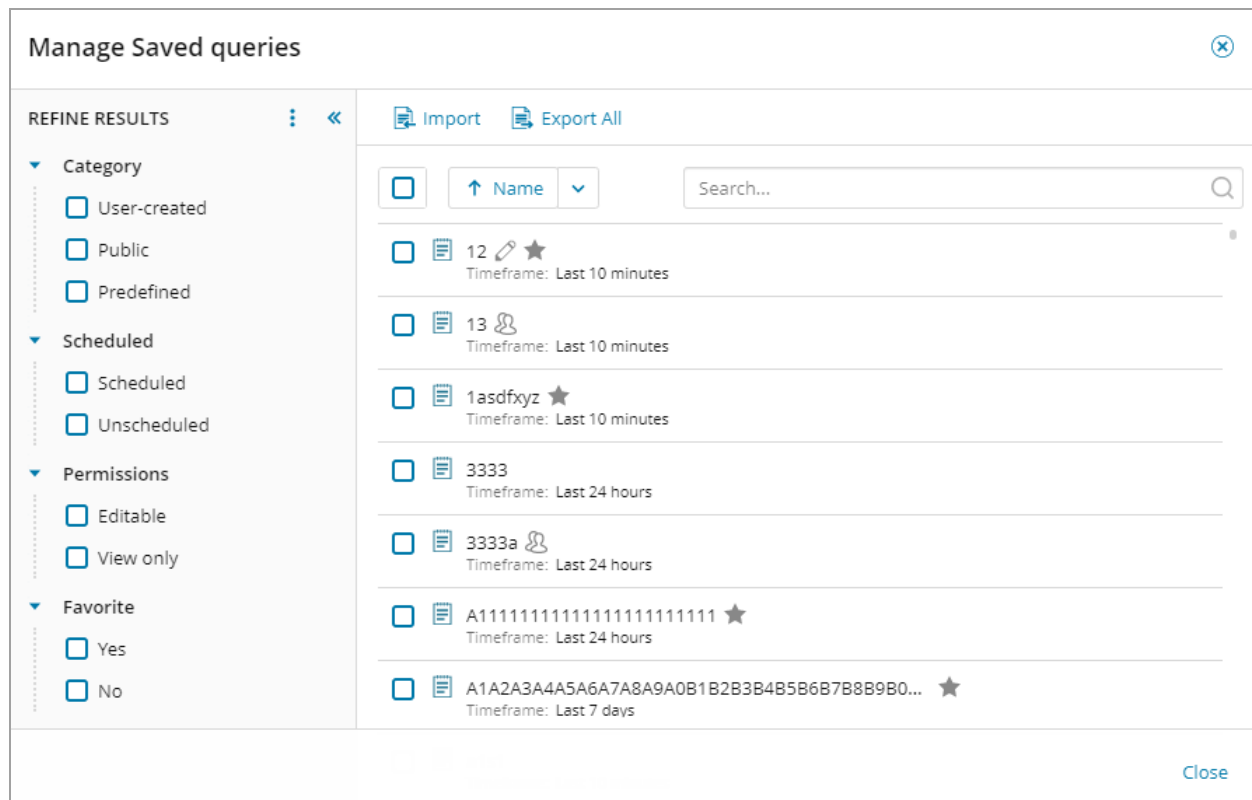
☒ Not Shared
This Query will be available only to you.

☐ Use only
Others users of SEM will be able to use this Query. Only you will be able to edit this Query.

☐ Allow editing
All users of SEM will be able to edit an delete this Query. This Query will be placed in Public folder. You will no longer be an owner of this Query.

Cancel
Save

- Click Export to export this query as a JSON file. To export more than one query, see [Import and export queries](#) for more information.
- Click Favorite to highlight this query with a star icon ★ and place it in the Favorites category.
- Click Manage queries option to open the Manage Saved queries window. This allows you to perform the above options on multiple queries by searching, sorting and selecting the queries. You can also [import and export filtered queries](#) from this window.

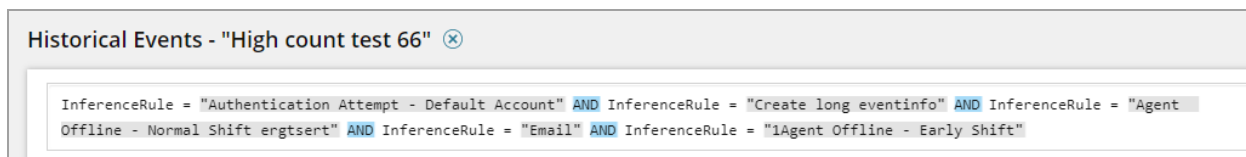


In this window, schedules (if created) and query timeframes are displayed.

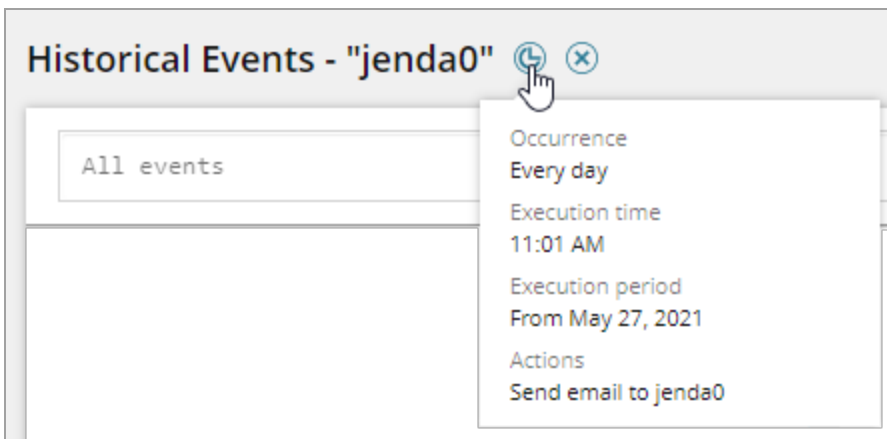
 The Manage Saved queries window is also available by clicking the gear icon at the top of the queries list.

Load queries

When you load a query, its name is displayed in the upper left and the query is displayed in the search query builder box.

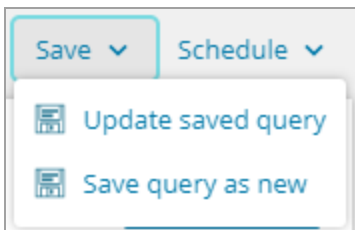


If there is a  icon after the name, this indicates that the query has a schedule. Move the cursor over this icon to display the schedule details.



If you make any changes to a saved search query, this is indicated by the **Edited**  icon after the name. Click this icon if you want to revert to the original query.

You can now save this updated search query as either a new query with a new name or update the existing query.



Click the Unload Current Query  icon if you do not want to use the loaded query. Note that the contents of the search query builder box are not automatically cleared by this action.

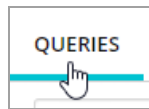
Search query tags and thresholds

You can [apply tags to queries](#) so they can be grouped for use with the Scheduled Query Severity and Scheduled Query Table Severity [widgets on the SEM dashboard](#). For example, you could apply the End User Monitoring tag to all queries relating to End User Monitoring.

Additionally, you can [apply threshold values](#) to search queries. This process allows you to set the number of occurrences for each evaluation that results in an event query result being deemed critical, warning or OK severity.

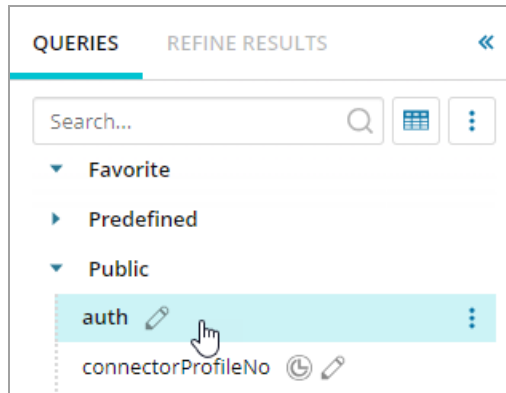
Apply tags to a query

1. In the toolbar, click Historical Events.
2. In the left column, click the Queries tab.



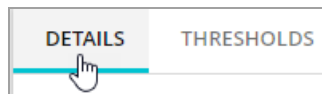
3. Maximize the targeted query category and select the query you want to edit.

For example:



i A query tagged with the Editable icon  can be edited, renamed and saved. A query tagged with the Use Only icon  can be used but not edited. You can copy and rename the query, which can be edited.

4. Click the vertical ellipsis  and select Edit in the drop-down menu.
5. In the Edit screen, ensure that the Details tab is selected.



6. Click Add tag and select the required tag or tags to apply to this query. Tags applied to the query are displayed above the Add tags link.

DETAILS
THRESHOLDS

Details

Name

Tags

Tags can be used to group queries for purposes of Dashboard overview widgets. [Learn more](#)

+ Add tag

☐ Linux/UNIX
☐ Manager
☒ Network Services
☐ Operating Systems
☐ Proxy Servers and Content Filters
☐ Routers/Switches
☐ System Scan Reporters
☐ VPN and Remote Access
☐ Windows

AUTHENTICATION

☐ Authentication

Cancel
Add

7. Click Add.

After you select one or more tags, specify the thresholds that determine whether event search results display as Critical, Warning or OK on the dashboard widgets.

Thresholds

You can apply threshold values to search queries to set the number of occurrences per evaluation (that is, when the query was last run) that result in an event query result being deemed critical, warning or OK severity.

DETAILS
THRESHOLDS

Thresholds

Thresholds are used to determine the severity level and colors on Dashboard overview widgets. [Learn more](#)

 Critical severity over ^ v result per evaluation (optional)

 Warning severity over ^ v result per evaluation (optional)

 Ok severity will be shown when there are any results per evaluation

 Warning severity under ^ v result per evaluation (optional)

 Critical severity under ^ v result per evaluation (optional)

Once you have set up tags and thresholds for a query, you can use this data to set up widgets on the SEM dashboard.

Widgets

The scheduled query widgets are [created](#) and [customized](#) in the same way as other [SEM Dashboard widgets](#).

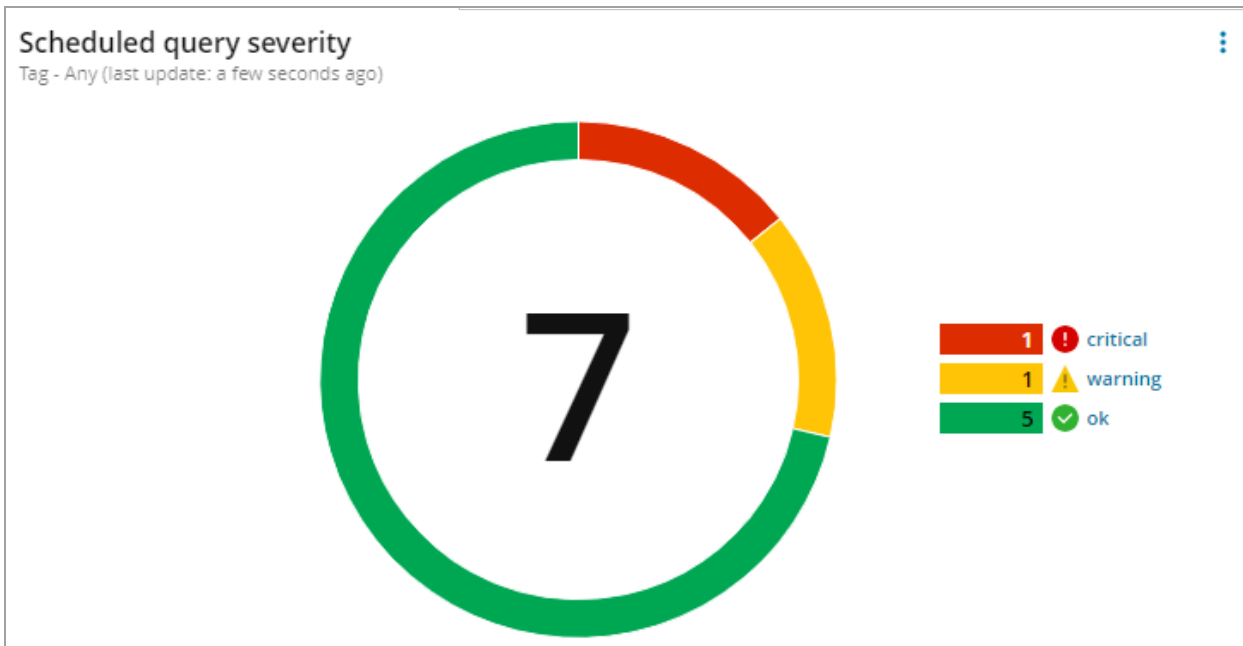
Scheduled Query Table Severity widget

The following widget has been customized to list all search queries that have returned one or more event within the most recent evaluation. It shows the number of occurrences and the time the query was last run.

Scheduled query severity overview (last update: 2 minutes ago)			
Severity	Search Name	Count of Events	Execution date
	connectorProfileNo	30	2022-10-17 01:25:04
	Daizy's query	30	2022-10-17 01:25:09
	Test123	16045	2022-10-17 05:34:55
	Test1f23	15792	2022-10-17 05:34:55
	test	15292	2022-10-17 06:29:55
	Copy	3015269	2022-10-17 02:16:54

Scheduled Query Severity widget

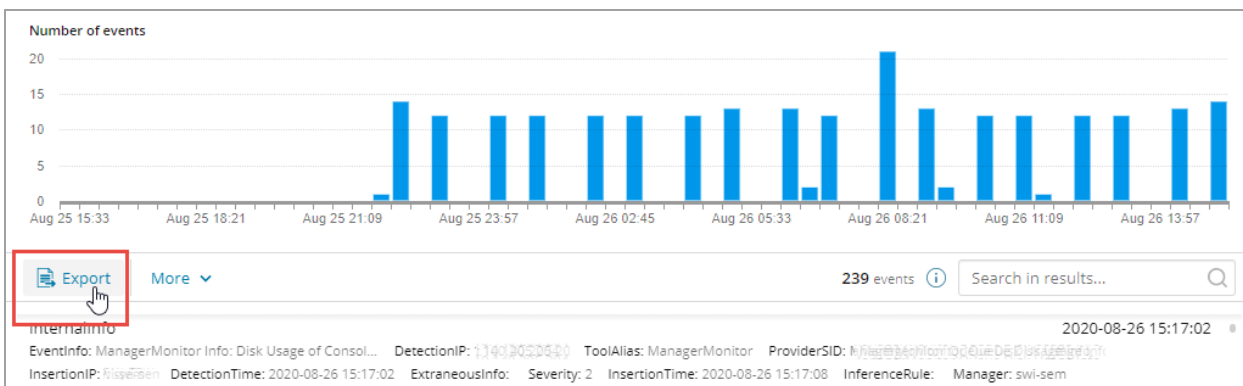
Click the red, yellow or green area of the query severity widget to display the corresponding query on the Historical Events page.



If more than one query is tagged, the Manage Saved queries window will display, listing all queries that apply to this severity level

Export historical search results

You can export logs from your historical event query to a CSV file. Once the search engine has returned the results of your query, click Export to download a CSV file to your local system.



You are asked to provide a file name and file path, or accept the default.

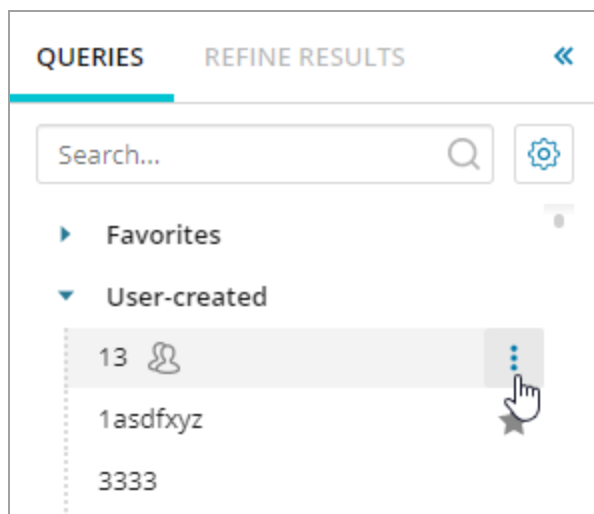
Import and export historical event queries

You can export search queries from SEM historical events in JSON format either as individual queries or by exporting multiple queries.

Export a single query

To export a single query:

1. On the SEM Console, click the Historical Events and Reports tab.
2. Select the queries tab and open the category containing the required query.
3. Move the cursor over the required query and click on the vertical ellipsis icon .



The Queries menu is displayed.

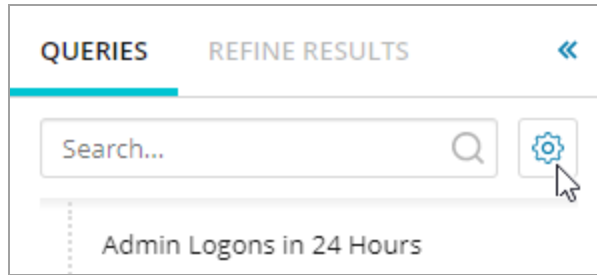
4. Click Export.
5. Enter a meaningful filename and click Save.

Export multiple queries

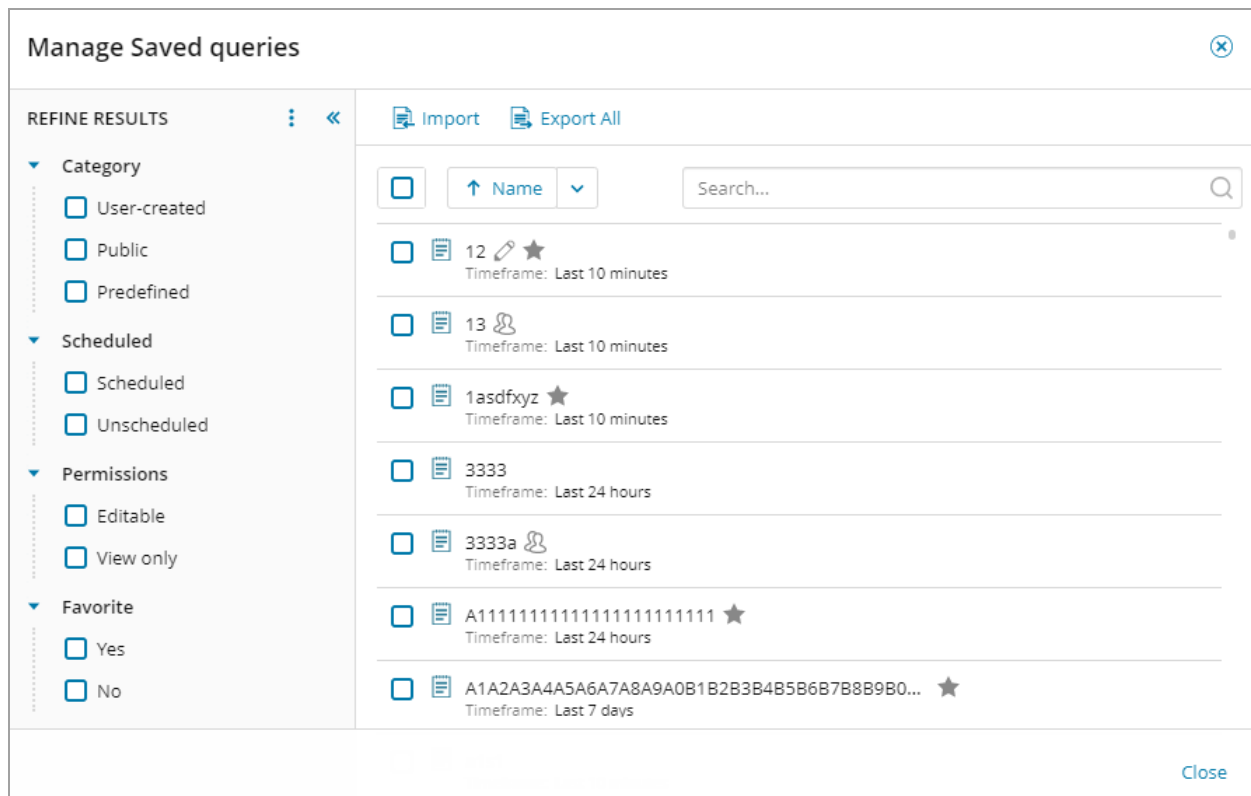
To export all search queries:

1. On the SEM Console, click the Historical Events and Reports tab.
2. Select the Queries tab.

- Click the gear icon at the top of the queries list.



- The Manage Saved queries window is displayed.



- Initially the options are Import and Export All. These change depending on how you proceed.

- To export all your queries, click Export All.
- To export a set of queries, use the checkboxes on the left to filter queries by category, whether scheduled or not, etc and select Export Filtered.
- To export specific queries use the checkboxes in front of the query names and click Export.

- Enter a meaningful filename and click Save.

Import queries

To import search queries that have been previously saved as a JSON file:

1. On the SEM Console, click the Historical Events and Reports tab.
2. Select the queries tab.
3. Click the gear icon at the top of the queries list.

The Manage Saved queries window is displayed.

4. Click Import.

The Import Queries window is displayed.

Import Queries

File import Queries selection Summary

File import

Import multiple Queries from a different SEM instance. Select an exported JSON file and import it into your SEM instance. Queries will be shown in **User-created** category. You will also be able to select which Queries from the file should be imported and solve any potential conflicts with Queries that already exist in your SEM instance.

Select JSON file

[Browse file](#) No file selected yet.

[Cancel](#) [Next >](#)

5. Click Browse file, navigate to the required JSON file, and click Open.
6. Click Next.

The queries contained in the selected JSON file are listed.

Import Queries

File import

Queries selection

Summary

Queries selection

☒

↑ Name

↓

Search...

☒

12

Timeframe: Last 10 minutes

☒

13

Timeframe: Last 10 minutes

☒

A11111111111111111111111111111111

Timeframe: Last 24 hours

☒

A1A2A3A4A5A6A7A8A9A0B1B2B3B4B5B6B7B8...

Timeframe: Last 7 days

☒

...

Cancel

< Back

Next >

- Filter out any queries you do not want to import by unchecking the boxes in front of the query names, then click Next.

The import process begins. The queries that are successfully imported are listed. Those that cannot be imported are shown along with the reasons why.

Administrator Guide: Security Event Manager

page 357

Import Queries

File import

Queries selection

Summary

Summary

Not imported

! 13

Name conflict

! 1asdfxyz

Name conflict

Imported successfully

✓ 12

✓ Copy of 3333

✓ mySuperSharedByMe

Ok

- When the import is complete, click OK to close the box. The queries will now be listed in the appropriate categories in the Queries column.

Set the live and historical event limits

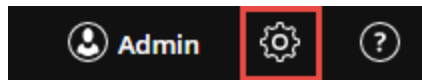
You can set the maximum number of events that populate the filters in your SEM Live Events and Historical Events viewers. This setting also applies to the dashboard widget showing event data.

The default setting for each is 10,000 events.

! On average, every 1,000 returned search results consumes approximately 100MB of RAM, which can increase up to 10GB for one search query if the threshold is set to the 100,000 maximum. Predictably, executing multiple search queries simultaneously will add additional strain to system resources and cause diminished performance.

To change the number of events that populate these filters:

- On the SEM Console, click the Settings button.



2. On the Settings page, click the Events Limits tab.
3. Click Live or Historic, depending on which set of events you want to set the limits for, and enter the number of search results..

You can enter between 100 and 10000000 (ten million). The default value is 100.

4. Click Save.
5. Restart the manager service for the new setting(s) to take place.

Configure the occurrence settings

By default, a condition must occur once to satisfy part of a rule. You can change this using the occurrence setting. For example, you can know if an occurrence happens five times in thirty seconds.

To apply occurrence settings for this part of the rule, click the  icon on the SEM rule builder tool bar.

Occurrence settings

Conditions must happen

1

^

v

times within

30

^

v

seconds

v

Applying to this part of the rule

 AttackBehavior occurred

Cancel

Save

If you change the number of times this condition occurs to satisfy this part of the rule, the window is expanded as shown below.

Occurrence settings

Conditions must happen

5

^

v

times within

30

^

v

seconds

v

Occurrence instance properties

Event instances must have following properties

+ Add condition

Occurrence time

☐ Set time when a rule won't trigger actions after rule was true

Applying to this part of the rule

 AttackBehavior occurred

occurs at least 5x in 30 sec

Cancel

Save

You can also specify additional conditions. For example the following would be true if the event occurred twice within ten minutes with the same DetectionIP.

Occurrence settings

Conditions must happen

2

↑

↓

times within

10

↑

↓

minutes

Occurrence instance properties

Event instances must have following properties

AttackBehavior

with same

DetectionIP

[+ Add condition](#)

Occurrence time

☐ Set time when a rule won't trigger actions after rule was true

Applying to this part of the rule

⚡ AttackBehavior occurred

[Cancel](#)
[Save](#)

You can additionally set a period that must elapse before this part of the rule can be triggered again by checking the Occurrence time box.

Edit the expressions

To change the expression for a rule part, click the  icon on the SEM rule builder tool bar. A popup window is displayed showing the components of the expression. For an entity, this will show two field: the entity name and whether or not the condition occurred. For an entity field, the following fields are displayed.

Rule is true when

⚡ AttackBehavior.Severity is equal to

5

⚙️

✏️

🗑️

+

+

Click or drag item from the left

And whole rule

occurs at least 1x in 30 sec

in 5

⚡ AttackBehavior

Severity

is equal to

Number

5

↑

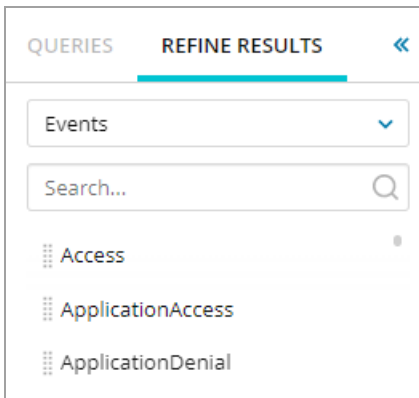
↓

[Cancel](#)
[Save](#)

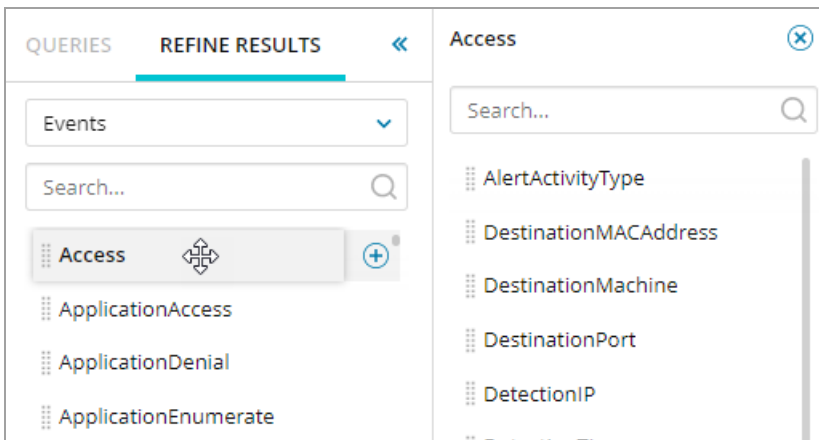
About the event types

The Historical Events view displays all normalized events in the Refined Results column. You can configure these events with the Policy commands.

To view all events, click the drop-down menu and select Events.



When you select an event, the corresponding normalized alerts display in the second column. For example, when you click Access, all access-related alerts display in the second column.



SEM includes five types of events. The following table lists each event type and their corresponding alerts.

Event type	Description
Asset events	Addresses the changing state of different types of enterprise assets, including software, hardware, and users. Asset event alerts indicate changes made to system configuration, software updates, patch applications, vulnerability information, and other system events.
Audit events	Address normal network activity that would not be considered an attack, compromise, or misuse of resources. Many audit alerts are associated with rules that can be used to threshold and escalate "normal" behavior into something that might be considered a security event.

Event type	Description
Incident events	Raise global enterprise-wide visibility in response to any issue detected by Rules. Incidents reflect serious issues that should be addressed. Because incidents are created by rules, any combination of malicious or suspicious traffic from any other single alert or combination of alerts can create an incident.
Internal events	Address SEM system operations. Any event generated by SEM relating to Active Response, SEM users, or SEM errors display as one of the many children. These alerts are for informational purposes only. They do not necessarily reflect conditions that should cause alarm. Events that might reflect potential issues with SEM are specifically marked for forwarding to SolarWinds.
Security events	Address network activity that is consistent with an internal or external attack, a misuse or abuse of resources, a resource compromise, resource probing, or other abnormal traffic that is noteworthy. Security events indicate aggressive behavior that might lead to an attack or resource compromise, or suspicious behavior that might indicate unauthorized information gathering. SEM infers some security events from is normally considered audit traffic, but it escalates the events from alert status based on thresholds that are defined by rules.

Asset events

Asset events address assets and asset scan results. They relate to the changing state of different types of enterprise assets, including software, hardware, and users.

Asset information can come from centralized directory service connectors. The information can also be scanned information from security scan connectors, including vulnerability assessment and patch management connectors. These alerts indicate changes made to system configurations, software updates, patch applications, vulnerability information, and other system events.

Listed below are all asset event alerts in alphabetical order.

AssetManagement

AssetManagement alerts gather non-realtime data about system assets (such as computer, software, and users). The data comes from various sources, including directory service connectors.

AssetManagement > MachineAsset

MachineAsset is a specific type of AssetManagement alert that indicates additions, removals, and updates (including software installation) of specific nodes that exist in the enterprise.

AssetManagement > MachineAsset > MachineAssetAdded

MachineAssetAdded alerts indicate a new presence of a node (host or network device) in the enterprise.

AssetManagement > MachineAsset > MachineAssetRemoved

MachineAssetRemoved alerts indicate the removal of a node (host or network device) from the enterprise.

AssetManagement > MachineAsset > MachineAssetUpdated

MachineAssetUpdated alerts indicate a change to an existing node (host or network device) in the enterprise, including new software and software patch installations on the node.

AssetManagement > MachineAsset > MachineAssetUpdated > SoftwareAssetUpdated

SoftwareAssetUpdated alerts indicate an attempted software change (including the application of a software patch) to an existing node (host or network device) in the enterprise, successful or failed.

AssetManagement > MachineAsset > MachineAssetUpdated > SoftwareAssetUpdated > SoftwareAssetPatched

SoftwareAssetPatched alerts indicate a successful application of a software patch to an existing node (host or network device) in the enterprise.

AssetManagement > MachineAsset > MachineAssetUpdated > SoftwareAssetUpdated > SoftwareAssetPatchFailed

SoftwareAssetPatchFailed alerts indicate a failed application of a software patch to an existing node (host or network device) in the enterprise.

AssetManagement > SoftwareAsset

SoftwareAsset is a specific type of AssetManagement alert that indicates additions, removals, and updates of specific software and software versions that exist in the enterprise.

AssetManagement > SoftwareAsset > SoftwareAssetAdded

SoftwareAssetAdded alerts indicate a new presence of an installation of specific software applications or operating systems in the enterprise.

AssetManagement > SoftwareAsset > SoftwareAssetAdded > SoftwareAssetVersionAdded

SoftwareAssetVersionAdded alerts indicate a new version installation of specific known software applications or operating systems in the enterprise.

AssetManagement > SoftwareAsset > SoftwareAssetRemoved

SoftwareAssetRemoved alerts indicate removals of specific software applications or operating systems from the enterprise.

AssetManagement > UserAsset

UserAsset is a specific type of AssetManagement alert that indicates additions, removals, and updates to users and user groups that exist in the enterprise.

AssetManagement > UserAsset > GroupAssetAdded

GroupAssetAdded alerts indicate a new presence of a user group in the enterprise.

AssetManagement > UserAsset > GroupAssetRemoved

GroupAssetRemoved alerts indicate the removal of a user group from the enterprise.

AssetManagement > UserAsset > GroupAssetUpdated

GroupAssetUpdated alerts indicate a change to a user group that exists in the enterprise, including group member additions and deletions.

AssetManagement > UserAsset > GroupAssetUpdated > GroupAssetMemberAdded

GroupAssetMemberAdded alerts indicate an addition of a user member to a user group that exists in the enterprise.

AssetManagement > UserAsset > GroupAssetUpdated > GroupAssetMemberRemoved

GroupAssetMemberRemoved alerts indicate a removal of a user member from a user group that exists in the enterprise.

AssetManagement > UserAsset > UserAssetAdded

UserAssetAdded alerts indicate a new presence of a user in the enterprise.

AssetManagement > UserAsset > UserAssetRemoved

UserAssetRemoved alerts indicate the removal of a user from the enterprise.

AssetManagement > UserAsset > UserAssetUpdated

UserAssetUpdated alerts indicate a change to a user that exists in the enterprise.

AssetScanResult

AssetScanResult contains alerts useful for data gathered from security scan results (reports). These alerts are commonly gathered from vulnerability assessment and patch management connectors.

AssetScanResult > ExposureFound

ExposureFound alerts indicate scan results that are not high risk but demonstrate configuration issues or potential risks. These alerts may indicate exposures that can potentially cause future exploits or have been common sources of exploits in the past, such as common open ports or host configuration issues.

AssetScanResult > VulnerabilityFound

VulnerabilityFound alerts indicate scan results that demonstrate high risk vulnerabilities. These alerts can indicate the presence of serious exposures that should be addressed and can represent significant risk of exploit or infection of enterprise assets.

GeneralAsset

GeneralAsset alerts are generated when a supported product outputs data that is not normalized into a specific alert, but known to be asset issue-related.

Audit events

Audit events are generally related to normal network activity that would not be considered an attack, compromise, or misuse of resources. Many of the audit alerts have rules that can be used to threshold and escalate “normal” behavior into something which may be considered a security event.

Listed below are all audit event alerts in alphabetical order.

AuthAudit

AuthAudit events are related to authentication and authorization of accounts and account containers, such as groups or domains. These alerts can be produced from any network node including firewalls, routers, servers, and clients.

AuthAudit > DomainAuthAudit

DomainAuthAudit events are authentication, authorization, and modification events related only to domains, subdomains, and account containers. These alerts are normally operating system related. However, they can be generated by any network device.

AuthAudit > DomainAuthAudit > NewDomainMember

NewDomainMember events occur when an account or account container is added to a domain. Usually, these additions are made by a user account with administrative privileges. Occasionally, a NewDomainMember alert will also occur when local system maintenance activity takes place.

AuthAudit > DomainAuthAudit > DeleteDomainMember

DeleteDomainMember events occur when an account or account container is removed from a domain. Usually, these changes are made by a user account with administrative privileges. Occasionally a DeleteDomainMember alert can also occur when local system maintenance activity takes place.

AuthAudit > DomainAuthAudit > ChangeDomainMember

A ChangeDomainMember alert occurs when an account or account container within a domain is modified. Usually, these changes are made by a user account with administrative privileges. Occasionally, a ChangeDomainMember alert can also occur due to local system maintenance activity.

AuthAudit > DomainAuthAudit > ChangeDomainMember > DomainMemberAlias

DomainMemberAlias events occur when an account or account container within a domain has an alias created, deleted, or otherwise modified. This event is uncommon and is used to track links between domain members and other locations in the domain where the member may appear.

AuthAudit > DomainAuthAudit > NewDomain

NewDomain events occur when a new trust relationship is created between domains, a new subdomain is created, or new account containers are created within a domain. Usually, these creations are done by a user account with administrative privileges.

AuthAudit > DomainAuthAudit > ChangeDomainAttribute

ChangeDomainAttribute events occur when a domain type is changed. These events are uncommon and usually provided by the operating system. Usually, these changes are made by a user account with administrative privileges. Occasionally, a ChangeDomainAttribute alert occurs when local system maintenance activity takes place.

AuthAudit > DomainAuthAudit > DeleteDomain

DeleteDomain events occur when a trust relationship between domains is removed, a subdomain is deleted, or account containers within a domain are deleted. These changes are usually performed by a user account with administrative privileges.

AuthAudit > GroupAudit

GroupAudit events are authentication, authorization, and modification events related only to account groups. These alerts are normally operating system related. However, they can be produced by any network device.

AuthAudit > GroupAudit > ChangeGroupAttribute

ChangeGroupAttribute events occur when a group type is modified. Usually, these changes are made by a user account with administrative privileges. Occasionally, a ChangeGroupAttribute alert will also occur when local system maintenance activity takes place.

AuthAudit > GroupAudit > DeleteGroup

DeleteGroup events occur when a new group of any type is deleted. These deletions are usually made by a user account with administrative privileges.

AuthAudit > GroupAudit > DeleteGroupMember

DeleteGroupMember events occur when an account or group is removed from a group. These changes are usually made by a user account with administrative privileges. Occasionally, a DeleteGroupMember alert will also occur when local system maintenance activity takes place.

AuthAudit > GroupAudit > NewGroup

NewGroup events occur when a new group of any type is created. These additions are usually made by a user account with administrative privileges.

AuthAudit > GroupAudit > NewGroupMember

NewGroupMember events occur when an account (or another group) is added to a group. These additions are usually made by a user account with administrative privileges. Occasionally, a NewGroupMember alert will also occur when local system maintenance activity takes place or a new user, machine, or service account is added to the group.

AuthAudit > MachineAuthAudit

MachineAuthAudit events are authentication, authorization, and modification events related only to computer or machine accounts. These alerts can be produced from any network node including firewalls, routers, servers, and clients. Normally, they are related to the operating system.

AuthAudit > MachineAuthAudit > MachineAuthTicketFailure

MachineAuthTicketFailure alerts reflect failed computer or machine account ticket events from network devices that use a ticket-based single-sign-on system (such as Kerberos or Windows domains). Each alert reflects the point on the network where the computer or machine was attempting a logon. In larger quantities, these alerts may reflect a potential issue with a computer or set of computers. As individual events, they are generally not a problem.

AuthAudit > MachineAuthAudit > MachineAuthTicket

MachineAuthTicket alerts reflect computer or machine account ticket events from network devices that use a ticket-based single-sign-on system (such as Kerberos or Windows domains). Each alert reflects the type of device the logon was intended for, along with all other relevant fields.

AuthAudit > MachineAuthAudit > MachineDisable

MachineDisable events occur when a machine account is actively disabled and/or when an account is forcibly locked out by the operating system or another authentication connector. These events are usually operating system related and could reflect a potential issue with a computer or set of computers.

AuthAudit > MachineAuthAudit > MachineEnable

MachineEnable alerts reflect the action of enabling a computer or machine account. These events are normally related to the operating system and triggers when a machine is 'enabled', normally by a user with administrative privileges.

AuthAudit > MachineAuthAudit > MachineLogoff

MachineLogoff alerts reflect computer or machine account logoff events from network devices (including network infrastructure devices, where appropriate). Each alert reflects the type of device from which the user was logging off. These alerts are usually normal events, but are tracked for consistency and auditing purposes.

AuthAudit > MachineAuthAudit > MachineLogonFailure

MachineLogonFailure alerts reflect failed computer or machine account logon events from network devices (including network infrastructure devices, when appropriate). Each alert reflects the point on the network where the computer or machine was attempting a logon. In larger quantities, these alerts can reflect a potential issue with a computer or set of computers. As individual events, they are generally not a problem.

AuthAudit > MachineAuthAudit > MachineLogon

MachineLogon events reflect computer or machine account logon events from network devices monitored (including network infrastructure devices, when appropriate). Each alert reflects the type of device that the logon was intended for, along with all other relevant fields. These events are normally related to the operating system.

AuthAudit > MachineAuthAudit > MachineModifyAttribute

MachineModifyAttribute events occur when a computer or machine type is changed. These events are uncommon and usually provided by the operating system.

AuthAudit > MachineAuthAudit > MachineModifyPrivileges

MachineModifyPrivileges events are created when a computer or machine's privileges are elevated or demoted based on their logon or activities they are performing. These events are uncommon.

AuthAudit > UserAuthAudit

UserAuthAudit events are authentication, authorization, and modification events that only apply to user accounts. These alerts can be produced from any network node including firewalls, routers, servers, and clients.

AuthAudit > UserAuthAudit > UserAuthTicketFailure

UserAuthTicketFailure alerts reflect failed user account ticket events from network devices that use a ticket-based single-sign-on system (such as Kerberos or Windows domains). Each alert reflects the point on the network where the user was attempting a logon. In larger quantities, these alerts may reflect a potential issue with a user or set of users. As individual events, they are generally not a problem.

AuthAudit > UserAuthAudit > UserAuthTicket

UserAuthTicket alerts reflect user account ticket events from network devices monitored that use a ticket-based single-sign-on system (such as Kerberos or Windows domains). Each alert reflects the type of device that the logon was intended for, along with all other relevant fields.

AuthAudit > UserAuthAudit > UserDisable

UserDisable events occur when a user account is actively disabled and/or when a user is forcibly locked out by the operating system or another authentication connector. These events are usually operating system related and can reflect a potential issue with a user or set of users.

AuthAudit > UserAuthAudit > UserEnable

UserEnable alerts reflect the action of enabling a user account. These events are normally related to the operating system and triggers when an account is unlocked after lockout due to unsuccessful logons and 'enabled' in the traditional sense.

AuthAudit > UserAuthAudit > UserLogoff

UserLogoff alerts reflect account logoff events from network devices (including network infrastructure devices). Each alert reflects the type of device from which the user was logging off. These alerts are usually normal events, but are tracked for consistency and auditing purposes.

AuthAudit > UserAuthAudit > UserLogon

UserLogon alerts reflect user account logon events from monitored network devices (including network infrastructure devices). Each alert reflects the type of device that the logon was intended for, along with all other relevant fields.

AuthAudit > UserAuthAudit > UserLogonFailure

UserLogonFailure alerts reflect failed account logon events from network devices (including network infrastructure devices). Each alert reflects the point on the network where the user was attempting a logon. In larger quantities, these alerts may reflect a potential issue with a user or set of users. As individual events they are generally not a problem.

With SolarWinds policy, you can configure combinations of this event to escalate to FailedAuthentication in the Security tree, reflecting the increase in severity of the event over several occurrences.

AuthAudit > UserAuthAudit > UserModifyAttribute

UserModifyAttribute events occur when a user type is changed. These events are uncommon and usually provided by the operating system.

AuthAudit > UserAuthAudit > UserModifyPrivileges

UserModifyPrivileges events are created when a user's privileges are elevated or demoted based on their logon or activities they are performing. These events are uncommon.

GeneralAudit

GeneralAudit alerts are generated when a supported product outputs data that has not yet been normalized into a specific alert, but is known to be audit-related.

MachineAudit

MachineAudit alerts track hardware or software status and modifications. These events are generally acceptable, but do indicate modifications to the client system that may be noteworthy.

MachineAudit > SoftwareInstall

SoftwareInstall alerts reflect modifications to the system at a software level, generally an operating system level (or equivalent, in the case of a network infrastructure device). These alerts are generated when a user updates a system or launches system-native methods to install third party applications.

MachineAudit > SoftwareInstall > SoftwareUpdate

SoftwareUpdate is a specific type of SoftwareInstall alert that reflects a more current version of software being installed to replace an older version.

MachineAudit > SystemScan

SystemScan alerts reflect information related to scheduled or on-demand scans of systems. These alerts are generally produced by anti-virus, patch management, and vulnerability assessment connectors. Additionally, these alerts indicate the start, finish, and information related to a scan.

MachineAudit > SystemScanInfo

SystemScanInfo is a specific type of SystemScan alert that reflects information related to a system scan. Most of these events can safely be ignored, as they are generally normal activity that does not reflect a failure or abnormal state.

MachineAudit > SystemScanStart

SystemScanStart is a specific type of SystemScan alert that indicates the initiation of a system scan.

MachineAudit > SystemScanStop

SystemScanStop is a specific type of SystemScan alert that indicates a system scan is completed. This activity is generally normal. However, in the error or failure state, a specific alert will be generated.

MachineAudit > SystemScanWarning

SystemScanWarning is a specific type of SystemScan alert that indicates a scan has returned a 'Warning' message, indicating an issue. These alerts may indicate scan issues that should be corrected for future scans.

MachineAudit > SystemStatus

SystemStatus alerts reflect general system state events. These events are generally normal and informational. However, they could potentially reflect a failure or issue which should be addressed.

MachineAudit > SystemStatus > SystemReboot

SystemReboot is a specific type of SystemStatus alert used to audit system restarts. This alert will only be generated if the system restart was normal and not a result of a crash or other failure condition.

MachineAudit > SystemStatus > SystemReboot > SystemShutdown

SystemShutdown is a specific type of SystemStatus alert used to audit system shutdowns, including both expected and unexpected shutdowns. If the shutdown was unexpected, the event detail notes the information provided by the connector related to the abnormality.

PolicyAudit

PolicyAudit events are used to track access, modification, scope change, and creation of authentication, domain, account, and account container policies. Many of these alerts reflect normal system traffic. Most PolicyAudit alerts are provided by the operating system.

PolicyAudit > NewAuthPolicy

NewAuthPolicy alerts occur when a new authorization or authentication package, process, or logon handler is applied to an item (usually an account or domain). In the operating system context, these events will often occur on boot, as the system initializes the appropriate authentication policies for itself.

PolicyAudit > PolicyAccess

PolicyAccess alerts reflect all levels of access to policy. These alerts mostly target domain, account, access, and logon policy modifications.

PolicyAudit > PolicyAccess > PolicyModify

PolicyModify alerts reflect all types of modifications to contained policies, both at a local and domain/account container level. In the context of a network infrastructure device, this would be a modification to access control lists or other similar policies on the device.

PolicyAudit > PolicyAccess > PolicyModify > DomainPolicyModify

DomainPolicyModify alerts are a specific type of PolicyModify alerts that reflect changes to domain and account container level policies. These types of policies are generally related to the operating system. These modifications are usually made by a user with administrative privileges. Occasionally, these changes can also be triggered by the local system.

PolicyAudit > PolicyAccess > PolicyScopeChange

PolicyScopeChange alerts are a specific type of PolicyAccess alert that reflect a new scope or assignment of policy to users, groups, domains, interfaces, or other items. In the context of the operating system, these events are usually describing elevation of user privileges according to predefined policies.

The process of this elevation is considered a scope change, as the user is being brought under a new scope of privileges appropriate to the type of access they are requesting (and being granted). These events may accompany or precede object or file opens, including other policies.

PolicyAudit > PolicyAccess > GroupPolicyModify

GroupPolicyModify alerts are specific PolicyAccess alerts used to describe modifications to account group policies. Usually, these modifications are made by a user with administrative privileges. Occasionally, these changes can also be triggered by the local system.

ResourceAudit

Members of the ResourceAudit tree are used to define different types of access to network resources. These resources may be network bandwidth/traffic, files, client processes or services, or other types of shared security-related 'commodities'.

ResourceAudit > FileAudit

FileAudit alerts track file activity on monitored network devices, usually through the Operating System or a Host-Based IDS. These events will note success or failure of the requested operation.

ResourceAudit > FileAudit > FileAuditFailure

FileAuditFailure alerts track failed file activity on monitored network devices, usually through the operating system or a host-based intrusion detection system (IDS). These events will note what requested operation failed.

ResourceAudit > FileAudit > FileRead

FileRead is a specific FileAudit alert generated for the operation of reading files (including reading properties of a file or the status of a file). These alerts may be produced by any connector used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileRead > FileExecute

FileExecute is a specific FileRead alert generated for the operation of executing files. These alerts may be produced by any connector used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileRead > FileDataRead

FileDataRead is a specific FileRead alert generated for the operation of reading data from a file (not just properties or status of a file). These alerts may be produced by any connector that is used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileWrite

FileWrite is a specific FileAudit alert generated for the operation of writing to a file (including writing properties of a file or changing the status of a file). These alerts may be produced by any connector that is used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileWrite > FileDataWrite

FileDataWrite is a specific FileWrite alert generated for the operation of writing data to a file (not just properties or status of a file). These alerts may be produced by any connector used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileWrite > FileCreate

FileCreate is a specific FileWrite alert generated for the initial creation of a file. These alerts may be produced by any connector that is used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileWrite > FileMove

FileMove is a specific FileWrite alert generated for the operation of moving a file that already exists. These alerts may be produced by any connector that is used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileWrite > FileDelete

FileDelete is a specific FileWrite alert generated for the deletion of an existing file. These alerts may be produced by any connector that is used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileWrite > FileAttributeChange

FileAttributeChange is a specific FileWrite alert generated for the modification of file attributes (including properties such as read-only status). These alerts may be produced by any connector that is used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileAudit > FileWrite > FileLink

FileLink is a specific FileWrite alert generated for the creation, deletion, or modification of links to other files. These alerts may be produced by any connector that is used to monitor the activity of file usage, including a host-based IDS and some operating systems.

ResourceAudit > FileHandleAudit

FileHandleAudit alerts are used to track file handle activity on monitored network devices, usually through low-level access to the operating system, either natively or with or a host-based IDS. These events note the success or failure of the requested operation.

ResourceAudit > FileHandleAudit > FileHandleClose

FileHandleClose is a specific FileHandleAudit alert generated for the closing of file handles. These alerts may be generated by a connector with low-level file access, such as an operating system or some host-based IDS.

ResourceAudit > FileHandleAudit > FileHandleCopy

FileHandleCopy is a specific FileHandleAudit alert generated for the copying of file handles. These alerts may be generated by a connector that has low-level file access, such as an operating system or some host-based IDS.

ResourceAudit > FileHandleAudit > FileHandleOpen

FileHandleOpen is a specific FileHandleAudit alert generated for the opening of file handles. These alerts may be generated by a connector that has low-level file access, such as an operating system or some host-based IDS.

ResourceAudit > FileSystemAudit

FileSystemAudit alerts reflect hardware to file system mapping events and usage of file system resources. These events are generally normal system activity, especially during system boot.

ResourceAudit > FileSystemAudit > MountFileSystem

MountFileSystem alerts are a specific type of FileSystemAudit that reflect the action of creating an active translation between hardware to a usable file system. These events are generally normal during system boot.

ResourceAudit > FileSystemAudit > UnmountFileSystem

UnmountFileSystem alerts are a specific type of FileSystemAudit that reflect the action of removing a translation between hardware and a usable file system. These events are generally normal during system shutdown.

ResourceAudit > NetworkAudit

Members of the NetworkAudit tree are used to define events centered on the usage of network resources and bandwidth.

ResourceAudit > NetworkAudit > ConfigurationTrafficAudit

ConfigurationTrafficAudit alerts reflect application-layer data related to the configuration of network resources. Included in ConfigurationTrafficAudit are protocols such as DHCP, BootP, and SNMP. ConfigurationTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of misconfiguration, inappropriate usage, attempts to enumerate or access network devices or services, attempts to access devices that are configured via these services, or other abnormal traffic.

ResourceAudit > NetworkAudit > CoreTrafficAudit

CoreTrafficAudit alerts reflect network traffic sent over core protocols. Events that are children of CoreTrafficAudit are related to the TCP, IP, UDP, and ICMP protocols. Events of this type and its children do not have any application-layer data.

Events placed in the parent CoreTrafficAudit alert are known to be a core protocol, but are not able to be further categorized based on the message provided by the connector.

ResourceAudit > NetworkAudit > CoreTrafficAudit > TCPTrafficAudit

TCPTrafficAudit alerts are a specific subset of CoreTrafficAudit alerts where the protocol is known to be TCP. TCPTrafficAudit alerts may indicate normal traffic inside the network, normal traffic pass-through, denied traffic, or other non-application TCP traffic that is not known to have any immediate attack basis.

ResourceAudit > NetworkAudit > CoreTrafficAudit > IPTrafficAudit

IPTrafficAudit alerts are a specific subset of CoreTrafficAudit alerts where the protocol is known to be IP. IPTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of spoofs, routing issues, or other abnormal traffic. Generally, for the abnormal traffic that is appropriate to escalate, a policy is defined to escalate this to an alert in the Security tree based on a threshold.

ResourceAudit > NetworkAudit > CoreTrafficAudit > UDPTrafficAudit

UDPTrafficAudit alerts are a specific subset of CoreTrafficAudit alerts where the protocol is known to be UDP. UDPTrafficAuditEvents may indicate normal traffic inside the network, normal traffic pass-through, denied traffic, or other non-application UDP traffic that is not known to have any immediate attack basis.

ResourceAudit > NetworkAudit > CoreTrafficAudit > ICMPTrafficAudit

ICMPTrafficAudit alerts are a specific subset of CoreTrafficAudit alerts where the protocol is known to be ICMP. ICMPTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of scans, floods, or other abnormal traffic. Generally, for the abnormal traffic that is appropriate to escalate, a policy is defined to escalate this to an alert in the Security tree based on a threshold.

ResourceAudit > NetworkAudit > CoreTrafficAudit > IPSecTrafficAudit

IPSecTrafficAudit alerts are a specific subset of CoreTrafficAudit alerts where the traffic is known to be related to non-application layer IPSec events (such as key exchanges). IPSecTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of misconfigured IPSec peers, problems with IPSec communication, or other abnormal traffic.

ResourceAudit > NetworkAudit > LinkControlTrafficAudit

LinkControlTrafficAudit alerts are generated for network events related to link level configuration. LinkControlTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of misconfiguration at the link level, inappropriate usage, or other abnormal traffic.

ResourceAudit > NetworkAudit > RoutingTrafficAudit

RoutingTrafficAudit alerts are generated for network events related to configuration of network routes using protocols such as IGMP, IGRP, and RIP. RoutingTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of misconfigured routing, unintended route configuration, or other abnormal traffic.

ResourceAudit > NetworkAudit > RoutingTrafficAudit > RIPTrafficAudit

RIPTrafficAudit alerts are a specific subset of RoutingTrafficAudit alerts where the protocol is known to be RIP. RoutingTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of misconfigured routing, unintended route configuration, or other abnormal traffic.

ResourceAudit > NetworkAudit > NamingTrafficAudit

NamingTrafficAudit alerts are generated for network events related to the naming of network resources and nodes, using protocols such as WINS and DNS. NamingTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of inappropriate DNS authority attempts, misconfiguration of naming services, and other abnormal traffic. In several cases, for traffic that is appropriate to escalate, a policy is defined to escalate this to an alert in the Security tree based on a threshold.

ResourceAudit > NetworkAudit > FileSystemTrafficAudit

FileSystemTrafficAudit alerts are generated for network events related to requests for remote file systems, using protocols such as SMB and NFS. FileSystemTrafficAudit alerts generally indicate normal traffic for networks that have remote file system resources, such as SMB and NFS shares. However, alerts of this type could also be symptoms of attempts to enumerate shares or services, misconfiguration of such resources, or other abnormal traffic. For networks that do not have remote file system resources, these alerts will generally indicate abnormal traffic.

ResourceAudit > NetworkAudit > ApplicationTrafficAudit

ApplicationTrafficAudit alerts reflect network traffic that is mostly or all application-layer data. Events that are children of ApplicationTrafficAudit are also related to application-layer resources. Events placed in the parent ApplicationTrafficAudit alert are known to be application-related, but are not able to be further categorized based on the message provided by the connector, or because they are uncommon and rarely, if ever, imply network attack potential.

ResourceAudit > NetworkAudit > ApplicationTrafficAudit > EncryptedTraffic

EncryptedTraffic alerts reflect application-layer traffic that is encrypted and intended for a secure host. Included in EncryptedTraffic alerts are client and server-side application events, such as key exchanges, that normally occur after the low-level session creation and handshaking have completed.

ResourceAudit > NetworkAudit > ApplicationTrafficAudit > EncryptedTraffic > EncryptedTrafficError

EncryptedTrafficError alerts are a specific subnet of EncryptedTraffic alerts that reflect problems while exchanging keys or data.

ResourceAudit > NetworkAudit > ApplicationTrafficAudit > MailTrafficAudit

MailTrafficAudit alerts reflect application-layer data related to mail services. Included in MailTrafficAudit are client and server mail events from protocols such as IMAP, POP3, and SMTP. MailTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of excessive mail usage, unintended mail traffic, abnormal command exchanges to a server, or generally abnormal traffic.

ResourceAudit > NetworkAudit > ApplicationTrafficAudit > WebTrafficAudit

WebTrafficAudit alerts reflect application-layer data related to web services. Included in WebTrafficAudit are client and server web events from web servers, web applications, content filter related events, and other web services. WebTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of inappropriate web usage, potential abuse of web services, or other abnormal traffic.

ResourceAudit > NetworkAudit > ApplicationTrafficAudit > TimeTrafficAudit

TimeTrafficAudit alerts reflect application-layer data related to network time configuration. Included in TimeTrafficAudit are protocols such as NTP and activities, such as detection of client-side network time updates. TimeTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of misconfiguration, inappropriate usage, or other abnormal traffic.

ResourceAudit > NetworkAudit > ApplicationTrafficAudit > TimeTrafficAudit > NTPTrafficAudit

NTPTrafficAudit alerts are a specific type of TimeTrafficAudit related to the Network Time Protocol.

ResourceAudit > NetworkAudit > ApplicationTrafficAudit > FileTransferTrafficAudit

FileTransferTrafficAudit alerts reflect application-layer data related to file retrieval and send to and from remote hosts. Included in FileTransferTrafficAudit are protocols such as TFTP and FTP. FileTransferTrafficAudit alerts generally indicate normal traffic. However, alerts of this type could also be symptoms of misconfiguration, inappropriate usage, attempts to enumerate or access file transfer services, attempts to access devices that require file transfer services for configuration, or other abnormal traffic.

ResourceAudit > NetworkAudit > PointToPointTrafficAudit

PointToPointTrafficAudit alerts reflect application-layer data related to point-to-point connections between hosts. Included in PointToPointTrafficAudit are encrypted and unencrypted point-to-point traffic.

ResourceAudit > NetworkAudit > PointToPointTrafficAudit > PPTPTrafficAudit

PPTPTrafficAudit alerts are a specific type of PointToPointTrafficAudit alerts that reflect application-layer encrypted peer-to-peer tunneling protocol (PPTP) activities. Included in PPTPTrafficAudit alerts are tunnel creation, tunnel deletion, session creation, and session deletion, among other PPTP-related events.

PPTPTrafficAudit alerts generally indicate normal traffic for networks that have PPTP-accessible devices on the network. However, alerts of this type could also be symptoms of inappropriate access, misconfiguration of the PPTP server or clients, other communications errors, or other abnormal traffic. For networks that do not have remote file system resources, these alerts will generally indicate abnormal traffic.

ResourceAudit > NetworkAudit > RemoteProcedureTrafficAudit

RemoteProcedureTrafficAudit alerts reflect application-layer data related to remote procedure services. Included in RemoteProcedureTrafficAudit are the traditional RPC services used to service remote logons and file shares. Also included are other services that require remote procedure access to complete authentication, pass data, or otherwise communicate.

RemoteProcedureTrafficAudit alerts generally indicate normal traffic for networks that have remote procedure services on their network. However, alerts of this type could also be symptoms of inappropriate access, misconfiguration of the remote procedure services, errors in the remote procedure calls, or other abnormal traffic.

ResourceAudit > NetworkAudit > RemoteProcedureTrafficAudit > RPCTrafficAudit

RPCTrafficAudit is a specific subset of RemoteProcedureTrafficAudit related to traditional RPC services, including portmapper. ResourceAudit > NetworkConnectionAudit NetworkConnectionAudit alerts are generated when a connection is initiated on a network client.

ResourceAudit > NetworkConnectionAudit > LANConnection

LANConnection is a specific type of NetworkConnectionAudit that reflects a successful connection on a physical network interface, such as an Ethernet card.

ResourceAudit > NetworkConnectionAudit > VPNConnection

VPNConnection is a specific type of NetworkConnectionAudit that reflects a successful connection to a remote VPN.

ResourceAudit > NetworkConnectionAudit > DialupConnection

DialupConnection is a specific type of NetworkConnectionAudit that reflects a successful connection through a traditional modem.

ResourceAudit > ObjectAudit

ObjectAudit alerts track special object activity on monitored network devices, usually through the operating system or a host-based IDS. Generally, objects are special types of system resources, such as registry items or user account databases. These objects may be actual files on the system, but are not necessarily human readable. These events will note success or failure of the requested operation.

ResourceAudit > ObjectAudit > ObjectAuditFailure

ObjectAuditFailure alerts track special object activity on monitored network devices, usually through the operating system or a host-based IDS. Generally, objects are special types of system resources, such as registry items or user account databases. These objects may be actual files on the system, but are not necessarily human readable. These events will note a failure of the requested operation.

ResourceAudit > ObjectAudit > ObjectDelete

ObjectDelete is a specific ObjectAudit alert generated for the deletion of an existing object. These alerts may be produced by any connector that is used to monitor the activity of file and object usage, including a host-based IDS and some operating systems.

ResourceAudit > ObjectAudit > ObjectLink

ObjectLink is a specific ObjectAudit alert generated for the creation, deletion, or modification of links to other objects. These alerts may be produced by any connector that is used to monitor the activity of file and object usage, including a host-based IDS and some operating systems.

ResourceAudit > ProcessAudit

ProcessAudit alerts are generated to track launch, exit, status, and other events related to system processes. These events usually reflect normal system activity. Process-related activity that may indicate a failure will be noted separately from normal activity in the alert detail.

ResourceAudit > ProcessAudit > ProcessStop

ProcessStop is a specific type of ProcessAudit alert that indicates a process stopped. ProcessStop usually reflects a normal application exit. However, in the event of an unexpected error, the abnormal state is noted.

ResourceAudit > ProcessAudit > ProcessStart

ProcessStart is a specific type of ProcessAudit alert that indicates a new process has been launched. ProcessStart usually reflects normal system activity.

ResourceAudit > ProcessAudit > ProcessWarning

ProcessWarning is a specific type of ProcessAudit alert that indicates a process has returned a Warning message that is not a fatal error and may not have triggered an exit of the process.

ResourceAudit > ProcessAudit > ProcessInfo

ProcessInfo is a specific type of ProcessAudit alert that reflects information related to a process. Most of these events can safely be ignored, as they are generally normal activity that does not reflect a failure or abnormal state.

ResourceAudit > ServiceAudit

ServiceAudit alerts are generated to track information and other events related to system components. These events usually reflect normal system activity. System service-related activity that may indicate a failure are noted separately from normal activity in the alert detail.

ResourceAudit > ServiceAudit > ServiceInfo

ServiceInfo is a specific type of ServiceAudit alert that reflects information related to a service. Most of these events can safely be ignored, as they are generally normal activity that does not reflect a failure or abnormal state.

ResourceAudit > ServiceAudit > ServiceStart

ServiceStart events are a specific type of ServiceAudit alert that indicates a new system service is starting.

ResourceAudit > ServiceAudit > ServiceStop

ServiceStop events are a specific type of ServiceAudit alert that indicates a system service is stopping. This activity is generally normal. However, in the event of an unexpected stop, the abnormal state will be noted.

ResourceAudit > ServiceAudit > ServiceWarning

ServiceWarning is a specific type of ServiceAudit alert that indicates a service has returned a Warning message that is not a fatal error and may not have triggered an exit of the service.

Incident events

Incident events reflect global enterprise-wide issues that should be raised for system-wide visibility. These alerts generally reflect serious issues that should be monitored and addressed. They are sub-categorized into different types of Incidents events that can provide more detailed information.

Because incident events are created by rules, any combination of malicious or suspicious traffic from any other single alert or combination of alerts can create an Incident event.

Listed below are all incident event alerts in alphabetical order.

HostIncident

HostIncident alerts reflect global enterprise-wide host system issues that should be raised for system-wide visibility. These alerts indicate issues on hosts that should be tracked and addressed, including security and administrative issues that apply specifically to host-based information.

HybridIncident

HybridIncident alerts reflect global enterprise-wide combined network and host system issues that should be raised for system-wide visibility. These alerts are used to indicate the combination of network and host-based issues that should be tracked and addressed, including security and administrative issues that span both network and host-based information.

NetworkIncident

NetworkIncident alerts reflect global enterprise-wide network system issues that should be raised for system-wide visibility. These alerts indicate network-based issues that should be tracked and addressed, including security and administrative issues that apply specifically to network-based information.

Internal events

Events that are a part of the InternalEvent node are related to the operation of the LEM system. Any events generated by the system relating to Active Response, Internal users, or Internal errors will appear under one of the many children.

These alerts are for informational purposes and do not necessarily reflect conditions that should cause alarm. Events that may reflect potential issues within the system are specifically marked for forwarding to SolarWinds.

Listed below are all internal event alerts in alphabetical order.

InternalAudit

InternalAudit alerts reflect attempted accesses and changes to components of the SEMsystem by existing SolarWinds users. Both successful and failed attempts will generate alerts.

InternalAudit > InternalAuditFailure

InternalAuditFailure is a specific type of InternalAudit alert that indicates failed audit information. These alerts are generated when a user fails to view or modify (including creation, update, and deletion) anything within the SolarWinds system. The alert includes the user, type of access, and item being accessed.

InternalAuditFailure events are uncommon and can indicate an attempted privilege escalation within the SEM system by unprivileged users.

InternalAudit > InternalAuditSuccess

InternalAuditSuccess is a specific type of **InternalAudit** alert that indicates successful audit information. These alerts are generated when a user successfully views or modifies (including creation, update, and deletion) anything within the SEM system. The alert will include the user, type of access, and item being accessed.

InternalCommands

InternalCommands alerts are only used internally with few exceptions. These alerts are used for sending commands through the system to complete active responses.

InternalCommands > InternalAgentToolCommand

InternalAgentToolCommand alerts are internal only. They are fired between managers and agents to manage the connector settings.

InternalCommands > InternalAgentFastPack

InternalAgentFastPack alerts are internal only. They are fired between managers and agents to configure updated connector signatures.

InternalFailure

Events that are a part of the **InternalFailure** tree reflect potential issues within the system. These alerts could reflect configuration issues, issues that cannot be resolved without contacting SolarWinds, and potential serious issues that also merit contacting SolarWinds.

InternalFailure > InternalError

InternalError alerts reflect configuration or install issues that should be reported to SolarWinds. These are generally internal errors related to connectors that may be producing unexpected log entries or conditions that were unexpected. These issues generally cannot be solved without contacting SolarWinds. However, they should not be fatal errors.

InternalFailure > InternalException

InternalException alerts reflect more serious problems within the system. These problems generally lie within the product implementation and may require a software update to eliminate. These alerts and their surrounding conditions should be reported to SolarWinds.

InternalFailure > InternalWarning

InternalWarning alerts are generally problems that can be solved by the user. Usually, these alerts are configuration related and may assist in debugging the underlying issue. **InternalWarning** alerts do not reflect internal problems within the system and thus should not be immediately reported to SolarWinds. However, they may assist with solving a technical support issue should the need arise.

InternalGeneralEvent

InternalGeneralEvent events are uncommon events used to track Internal information that has not been placed into a more specific InternalEvent. Events of the InternalFailure family providing more information will be generated in addition to this event, if the event is serious.

InternalInfo

Events within the InternalInfo family are related to events that occur within the system. Generally, these informational alerts are confirming or reporting normal activity, such as user updates, user logons, policy updates, and agent connection-related events.

InternalInfo > InternalAgentOffline

InternalAgentOffline alerts reflect detection of an agent disconnect to its manager. These alerts occur when the manager detects that the agent closed the connection. This may be due to network down time of the agent or the agent service shutting down.

InternalInfo > InternalAgentOnline

InternalAgentOnline alerts reflect successful connection of agents to their respective managers. These alerts occur when an agent initiates successful communication with the manager. This can be due to network down time of the manager or agent or due to an update of the targeted agent.

InternalInfo > InternalDuplicateConnection

InternalDuplicateConnection alerts occur when an agent attempts to connect to their manager more than once. These alerts are usually triggered by network issues on the agent end due to a possible asynchronous disconnection detection (for example, the manager was not able to detect the agent went offline, but the agent service was restarted). This issue can usually be resolved by stopping the agent service, waiting for the InternalAgentOffline alert, and then restarting the agent service.

InternalInfo > InternalInvalidConnection

InternalInvalidConnection alerts occur when an agent that the manager recognizes, but cannot communicate with, attempts to connect. These alerts usually reflect agents that are missing an update that was applied to the manager.

Ensure that the indicated agent is upgraded to the same release version of the system that is installed on your manager. If this alert persists, uninstall and reinstall the agent triggering the alert. This will force the Agent to re-initialize connection to the manager.

InternalInfo > InternalInvalidInstallation

InternalInvalidInstallation alerts occur in the unlikely case that the manager can communicate with the agent, but there are errors detected in the manager-to-agent relationship. These alerts are very uncommon, but may be triggered during an upgrade process.

Ensure that the targeted agent is upgraded to the same release version of the system installed on your manager. If this alert persists, uninstall and reinstall the agent triggering the alert. This will force the agent to re-initialize connection to the manager.

InternalInfo > InternalLicenseMaximum

InternalLicenseMaximum alerts reflect an attempt to add more agents to a manager that exceed the manager license tier. The number of agents that can be added is a hard limit that the manager stores and this limit is also enforced by the console. If more licenses are required, contact SolarWinds Sales for an update.

InternalInfo > InternalNewToolData

InternalNewToolData alerts generally reflect issues related to connectors with unexpected log entries or other unexpected conditions. These issues, although not fatal, generally cannot be solved without contacting SolarWinds.

InternalInfo > InternalPolicyConfiguration

InternalPolicyConfiguration alerts reflect the successful or unsuccessful attempts to update the policy on a given manager. These alerts are generated after the policy is successfully installed to the manager or after an error is detected. Generally, an error in updating the policy will also produce an alert from the InternalFailure family, providing more information.

InternalInfo > InternalToolOffline

InternalToolOffline alerts reflect a successful stop of an Internal tool. These alerts are generated after a connector stops the log file reader that was created when the connector was brought online. Generally, an error in an attempt to stop a connector will produce an alert from the InternalFailure family, providing more information.

InternalInfo > InternalToolOnline

InternalToolOnline alerts reflect the successful startup of an internal tool. These alerts are generated after a connector has successfully created a log file reader and has begun the reading process. Generally, an error in an attempt to start a connector produces an alert from the InternalFailure family, providing more information.

InternalInfo > InternalUnknownAgent

InternalUnknownAgent alerts occur when an agent that the manager does not recognize attempted to connect. Commonly, this alert is caused by removing the agent from the console before removing the agent service on the client.

These alerts may also be triggered during an upgrade process. In this case, they may reflect agents that are not up to date. This issue can usually be resolved by uninstalling and reinstalling the agent triggering the alert. This will force the agent to re-initialize connection to the manager.

InternalInfo > InternalUnsupportedAgent

InternalUnsupportedAgent alerts are generated when a valid agent connects and has not been upgraded to the same release version as the manager. The targeted agent failed to properly negotiate its connection or respond to a query, and has been assumed to be missing a required feature.

Ensure that the targeted agent is upgraded to the same SolarWinds release version that is installed on your manager. If this alert persists, uninstall and reinstall the agent triggering the alert. This will force the agent to re-initialize its connection to the manager.

InternalInfo > InternalUserLogoff

InternalUserLogoff alerts are generated when a user logs off or is disconnected from the console.

InternalInfo > InternalUserLogon

InternalUserLogon alerts are generated when a user successfully completes the logon process to a manager using the console. Failed log-on attempts are produced in a separate InternalUserLogonFailure alert.

InternalInfo > InternalUserLogonFailure

InternalUserLogonFailure alerts are generated when a user completes the initialization of a connection to the console, but enters an incorrect user name and/or password.

InternalInfo > InternalUserUpdate

InternalUserUpdate alerts are generated when a user is modified and the update is sent to the manager, or when the update has failed to apply. These updates include change or addition of an email address, change or addition of a pager, and change or addition of blocked alerts from selected agents. Generally, an error in updating a user will also produce an alert from the InternalFailure family.

InternalPolicy

InternalPolicy alerts reflect information related to correlation rules. These alerts indicate that a rule was triggered, either in test mode or under normal operating conditions.

InternalPolicy > InternalTestRule

InternalTestRule alerts reflect rule activity where a correlation rule is triggered and is set in Test mode. It indicates the trigger of the rule and includes an enumeration of what actions would take place (if any) if the rule was fully enabled. To remove a rule from Test mode, clear the Test checkbox for the rule in the Rule Builder.

InternalPolicy > InternalRuleFired

InternalRuleFired alerts reflect rule activity, specifically where a correlation rule has triggered. It indicates the trigger of the rule and includes an enumeration of what actions were triggered in response to the correlation.

Security events

Security events are generally related to network activity that is consistent with:

- Internal or external attacks
- Misuse or abuse of resources
- Resource compromise, resource probing, or other abnormal traffic that is noteworthy

Security events indicate aggressive behavior that may lead to an attack or resource compromise, or suspicious behavior that may indicate unauthorized information gathering. SEM infers some security events from what is normally considered audit traffic, but it escalates the events to alert status based on thresholds that are defined by rules.

Listed below are all security event alerts in alphabetical order.

AttackBehavior

Events that are children of AttackBehavior are generally related to network activity that may be consistent of an attack, misuse or abuse of resources, a resource compromise, or other abnormal behavior that should be considered indicative of a serious security event.

AttackBehavior > InferredAttack

InferredAttack alerts are reserved AttackBehavior alerts used for describing attacks that are a composite of different types of alerts. These events will be defined and inferred by policy.

AttackBehavior > ResourceAttack

Members of the ResourceAttack tree are used to define different types of malicious or abusive access to network resources, where these resources may be network bandwidth/traffic, files, client processes or services, or other types of shared security-related commodities.

AttackBehavior > ResourceAttack > NetworkAttack

Members of the NetworkAttack tree are used to define events centered on malicious or abusive usage of network bandwidth and traffic. These events include access to network resources, relaying attacks through network resources, or denial of service behavior on network resources.

AttackBehavior > ResourceAttack > NetworkAttack > Access

Children of the Access tree define events centered on malicious or abusive usage of network bandwidth or traffic where the intention or result is inappropriate or abusive access to network resources.

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess

ApplicationAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources where the related data is mostly or all application-layer.

Generally, ApplicationAccess alerts reflect attempted exploitation of weaknesses in server or client software, or information that is restricted or prohibited by device access control or policy. These alerts are generally provided by network-based intrusion detection systems. In some cases, network infrastructure devices (such as firewalls or proxy servers) may also provide them.

Events placed in the parent ApplicationAccess alert are known to be application-related, but not able to be further categorized based on the message provided by the connector or because they are uncommon.

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > DataBaseAccess

DataBaseAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through the application-layer database traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in database server or client software. These alerts are generally provided by network-based intrusion detection systems, the database server, or the client software.

The appropriate response to these alerts may require:

- Improving the access control of database servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to database servers or clients
- Removing the database service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > FileTransferAccess

FileTransferAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer file transfer traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in file transfer server or client software. These alerts are generally provided by network-based intrusion detection systems, file transfer server, or the client software.

The appropriate response to these alerts may include:

- Improving the access control of file transfer servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to file transfer servers or clients
- Removing the file transfer service or client application related to this event.

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > FileTransferAccess > FTPFileAccess

FTPFileAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to file systems of resources through application-layer file transfer traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in file transfer server or client software with the intent of information gathering or low-level file system access of the server or client. These alerts are generally provided by network-based intrusion detection systems, file transfer server, or the client software.

The appropriate response to these alerts may require:

- Improving the access control of file transfer servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to file transfer servers or clients
- Removing the file transfer service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > FileTransferAccess > FTPInvalidFormatAccess

FTPInvalidFormatAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer file transfer traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in file transfer server or client software with the intent of information gathering or low-level access to the server or client. These attacks are always abnormal traffic that the file transfer server or client is not prepared to respond to.

Attacks such as buffer overflows may also result in the server or client software or system being halted. These alerts are generally provided by network-based intrusion detection systems, file transfer server, or the client software.

The appropriate response to these alerts may include:

- Improving the access control of file transfer servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to file transfer servers or clients
- Removing the file transfer service or client application related to this event.

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > FileTransferAccess > FTPCommandAccess

FTPCommandAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer file transfer traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in file transfer server software with the intent of information gathering or low-level access to the server or client. These attacks are always abnormal command traffic that the file transfer server is not prepared to respond to, but may provide access to (such as debug or legacy commands). These alerts are generally provided by network-based intrusion detection systems, file transfer server, or the client software.

The appropriate response to these alerts may include:

- Improving the access control of file transfer servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to file transfer servers or clients
- Removing the file transfer service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > MailAccess

MailAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer mail transfer, retrieval, or service traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in mail-related server or client software. These alerts are generally provided by network-based intrusion detection systems, file transfer server, or the client software.

The appropriate response to these alerts may include:

- Improving the access control of file transfer servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to file transfer servers or clients
- Removing the file transfer service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > MailAccess > MailTransferAccess

MailTransferAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer mail transfer traffic.

Generally, these alerts will reflect attempted exploitation of weaknesses in SMTP server software. These alerts are generally provided by network-based intrusion detection systems, or the SMTP server software .

The appropriate response to these alerts may include:

- Improving the access control of the SMTP server (such as restriction by IP address and/or user name to ensure only trusted clients are connecting, especially for SMTP servers that relay mail for external or remote entities)
- Applying updates or patches to SMTP servers
- Removing the SMTP server related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > MailAccess > MailTransferAccess > SMTPInvalidFormatAccess

SMTPInvalidFormatAccess alerts reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through application-layer mail transfer traffic.

Generally, these alerts will reflect attempted exploitation of weaknesses in SMTP server software with the intent of information gathering or low-level access to the server. These attacks are always abnormal traffic that the SMTP server is not prepared to respond to; attacks, such as buffer overflows, may also result in the server software or system being halted. These alerts are generally provided by network-based intrusion detection systems, or the SMTP server software.

The appropriate response to these alerts may include:

- Improving the access control of the SMTP server (such as restriction by IP address or user name to ensure only trusted clients are connecting, especially for SMTP servers that relay mail for external/remote entities)
- Applying updates or patches to SMTP servers
- Removing the SMTP server related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > MailAccess > MailTransferAccess > SMTPInvalidFormatAccess > SmailAccess

SmailAccess alerts reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through application-layer mail transfer traffic.

Generally, these alerts will reflect attempted exploitation of weaknesses in SMTP server software with the intent of information gathering or low-level access to the server. These attacks are always abnormal traffic that the SMTP server is not prepared to respond to; they may also result in the server software or system being halted. The smail attack specifically attempts to execute applications resulting in compromise of the SMTP server system.

These alerts are generally provided by network-based intrusion detection systems, or the SMTP server software.

The appropriate response to these alerts may include:

- Improving the access control of the SMTP server (such as restriction by IP address or user name to ensure only trusted clients are connecting, especially for SMTP servers that relay mail for external/remote entities)
- Applying updates or patches to SMTP servers
- Removing the SMTP server related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > MailAccess > MailTransferAccess > SMTPCommandAccess

SMTPCommandAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer mail transfer traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in SMTP server software with the intent of information gathering or low-level access to the server. These attacks are always abnormal command traffic that the SMTP server is not prepared to respond to, but may provide access to (such as debug or legacy commands).

These alerts are generally provided by network-based intrusion detection systems, or the SMTP server software.

The appropriate response to these alerts may include:

- Improving the access control of the SMTP server (such as restriction by IP address or user name to ensure only trusted clients are connecting, especially for SMTP servers that relay mail for external/remote entities)
- Applying updates or patches to SMTP servers
- Removing the SMTP server related to this event.

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > MailAccess > MailDeliveryAccess

MailDeliveryAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer mail retrieval traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in mail retrieval related server or client software—the mail delivery agent (MDA) or mail user agent (MUA).

These alerts are generally provided by network-based intrusion detection systems, or the SMTP server software.

The appropriate response to these alerts may include:

- Improving the access control of the SMTP server (such as restriction by IP address or user name to ensure only trusted clients are connecting, especially for SMTP servers that relay mail for external/remote entities)
- Applying updates or patches to SMTP servers
- Removing the SMTP server related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > MailAccess > MailServiceAccess

MailServiceAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer mail service traffic.

Generally, these alerts reflect attempted exploitation of weaknesses in mail service-related server or client software, including services such as mailing list software, spam filters, email redirection software, and other mail filtering software.

These alerts are generally provided by network-based intrusion detection systems, mail service, or client software.

The appropriate response to these alerts may include:

- Improving the access control of mail services or servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to mail services or clients
- Removing the mail service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > MailAccess > MailServiceAccess > MajordomoAccess

MailServiceAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer mail service traffic. Generally, these alerts reflect attempted exploitation of weaknesses in Majordomo, which is a specific type of mailing list software.

These alerts are generally provided by network-based intrusion detection systems or mail service. Appropriate response to these alerts may include:

- Improving the access control of mail services or servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to the mail service, or the removal of the mail service related to this event.

Generally, the most appropriate response will be updates or patches that can be retrieved from the Majordomo web site or your operating system vendor.

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > NewsAccess

NewsAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer news traffic (over protocols such as NNTP). Generally, these alerts reflect attempted exploitation of weaknesses in the news server or client software.

These alerts are generally provided by network-based intrusion detection systems, news server, or client software.

The appropriate response to these alerts may include:

- Improving the access control of news servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)

Applying updates or patches to news servers or clients

- Removing the news service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > PrinterAccess

PrinterAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer remote printer traffic. Generally, these alerts reflect attempted exploitation of weaknesses in the remote printer server or client software.

These alerts are generally provided by network-based intrusion detection systems, remote printer server, or client software.

The appropriate response to these alerts may include:

- Improving the access control of remote printer servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote printer servers or clients
- Removing the remote printer service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess

WebAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic. Generally, these alerts reflect attempted exploitation of weaknesses in the web server or client software.

These alerts are generally provided by network-based intrusion detection systems, web server, or client software.

The appropriate response to these alerts may include:

- Improving the access control of web servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)

- Applying updates or patches to web servers and/or clients
- Removing the web service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPClientAccess

HTTPClientAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic where the information flow is from server to client. Generally, these alerts reflect attempted exploitation of weaknesses in the client software or abuse and/or misuse of resources from clients.

These alerts are generally provided by network-based intrusion detection systems, the web client software, proxy servers, content filters, or firewalls with the capability to monitor incoming web traffic.

The appropriate response to these alerts may include:

- Applying updates or patches to web client software
- Restricting incoming/outgoing web requests/responses to reflect inappropriate or abusive access

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPClientAccess > FraudulentCertificateAccess

FraudulentCertificateAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic where the information flow is from server to client. Generally, these alerts reflect attempted exploitation of weaknesses in the client software through fraudulent certificates. The intent of these attacks may be to forge certificates that convince the client that the site is trusted, when in fact it is not, passing data along with those certificates that may be inappropriate or contain exploits.

These alerts are generally provided by network-based intrusion detection systems, the web client software, proxy servers, content filters, or firewalls with the capability to monitor incoming web traffic.

The appropriate response to these alerts may include:

- Applying updates or patches to web client software
- Restricting incoming/outgoing web requests/responses to reflect the abusive access

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPClientAccess > ProhibitedHTTPControlAccess

ProhibitedHTTPControlAccess alerts reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through application-layer WWW traffic in which the information flow is from server to client. Generally, these alerts will reflect attempted exploitation of weaknesses in the client software or abuse or misuse of resources from clients through client controls such as ActiveX and Java.

These alerts are generally provided by network-based intrusion detection systems, the web client software itself, proxy servers, content filters, or firewalls with capability to monitor incoming web traffic.

The appropriate response to these alerts may include:

- Applying updates or patches to web client software
- Restricting incoming/outgoing web requests/responses to reflect inappropriate or abusive access

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPServerAccess

HTTPServerAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic where the information flow is from client to server. Generally, these alerts will reflect attempted exploitation of weaknesses in the server software or abuse or misuse of server resources.

These alerts are generally provided by network-based intrusion detection systems, web server or service software, or firewalls with the capability to monitor incoming/outgoing web traffic.

The appropriate response to these alerts may include:

- Improving the access control of web servers (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to web servers, services, or clients
- Removing the web service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPServerAccess > HTTPApplicationAccess

HTTPApplicationAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic in which the information flow is from client to server. Generally, these alerts reflect attempted exploitation of weaknesses in applications running on top of the server software, such as PHP, CGI, administrative sites, and other application services.

These alerts are generally provided by network-based intrusion detection systems, the web server, the service software, or firewalls with capability to monitor incoming/outgoing web traffic.

The appropriate response to these alerts may include:

- Improving the access control of web servers or the service itself (such as restriction by IP address or user name to ensure only trusted clients are connecting)

- Applying updates or patches to web servers, services, or clients
- Removing the web service application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPServerAccess > HTTPApplicationAccess > HTTPAdministrationAccess

HTTPAdministrationAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic in which the information flow is from client to server. Generally, these alerts reflect attempted exploitation of weaknesses in applications run on top of server software that are related to remote administration of sites, services, or systems.

These alerts are generally provided by network-based intrusion detection systems, web server, service software, or firewalls with capability to monitor incoming or outgoing web traffic.

The appropriate response to these alerts may include:

- Improving the access control of web servers or the service (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to web servers, services, administrative sites, or clients
- Removing the web service application or administrative site related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPServerAccess > HTTPApplicationAccess > HTTPDynamicContentAccess

HTTPDynamicContentAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic in which the information flow is from client to server. Generally, these alerts reflect attempted exploitation of weaknesses in applications running on top of the server software that generate dynamic content, such as PHP, CGI, and ASP.

These alerts are generally provided by network-based intrusion detection systems, web server, service software, or firewalls with capability to monitor incoming or outgoing web traffic.

The appropriate response to these alerts may include:

- Improving the access control of web servers or the service (such as restriction by IP address or user name to ensure only trusted clients are connecting)
- Applying updates or patches to web servers, services, dynamic content, and/or clients
- Removing the web service application or dynamic content related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPServerAccess > HTTPApplicationAccess > HTTPFileRequestAccess

HTTPFileRequestAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic in which the information flow is from client to server. Generally, these alerts reflect attempted exploitation of weaknesses in applications running on top of server software related to remote administration of sites, services, and/or systems with the intent of information gathering or low-level file system access of the server or client.

These alerts are generally provided by network-based intrusion detection systems, web server, service software, and/or firewalls with capability to monitor incoming/outgoing web traffic.

The appropriate response to these alerts may include:

- Improving the access control of web servers or the service (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to web servers, services, and/or clients
- Removing the web service application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPServerAccess > HTTPApplicationAccess > HTTPServiceAccess

HTTPServiceAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer WWW traffic where the information flow is from client to server. Generally, these alerts reflect attempted exploitation of weaknesses in applications running on top of server software related to remote services such as printing or console access.

These alerts are generally provided by network-based intrusion detection systems, web server, service software, and/or firewalls with the capability to monitor incoming/outgoing web traffic.

The appropriate response to these alerts may include:

- Improving the access control of web servers or the service (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to web servers, services, and/or clients
- Removing the web service application or site related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > WebAccess > HTTPServerAccess > HTTPInvalidFormatAccess

HTTPInvalidFormatAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer web traffic in which the information flow is from client to server. Generally, these alerts will reflect attempted exploitation of weaknesses in web server software with the intent of information gathering or low-level access to the server. These attacks are always abnormal traffic that the web server is not prepared to respond to; attacks, such as buffer overflows, may also result in the server software or system being halted.

These alerts are generally provided by network-based intrusion detection systems, web server, service software, and/or firewalls with the capability to monitor incoming/outgoing web traffic.

The appropriate response to these alerts may include

- Improving the access control of the web server (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to web servers or services
- Removing the web server related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > NamingAccess

NamingAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer naming service traffic (using protocols such as DNS and WINS). Generally, these alerts will reflect attempted exploitation of weaknesses in the naming server or client software.

These alerts are generally provided by network-based intrusion detection systems, naming server, or the client software.

The appropriate response to these alerts may include:

- Improving the access control of name servers (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to naming servers and/or clients
- Removing the naming service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > RemoteConsoleAccess

RemoteConsoleAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through application-layer remote console service traffic (services such as telnet, SSH, and terminal services). Generally, these alerts reflect attempted exploitation of weaknesses in the remote console server or client software.

These alerts are generally provided by network-based intrusion detection systems, remote console server, or the client software.

The appropriate response to these alerts may include:

- Improving the access control of remote console servers (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote console servers and/or clients
- Removing the remote console service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > ApplicationAccess > TimeAccess

TimeAccess alerts reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through application-layer remote time service traffic (using protocols such as NTP). Generally, these alerts will reflect attempted exploitation of weaknesses in the remote time server or client software.

These alerts are generally provided by network-based intrusion detection systems, the time server, or client software itself.

The appropriate response to these alerts may include:

- Improving the access control of remote time servers (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote time servers and/or clients
- Removing the remote time service or client application related to this event.

AttackBehavior > ResourceAttack > NetworkAttack > Access > ConfigurationAccess

ConfigurationAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through resource configuration traffic (using protocols such as DHCP, BootP, and SNMP). Generally, these alerts reflect attempted exploitation of weaknesses in the configuration server or client software or attempts to gain system-level access to configuration servers. In the case of SNMP and similar configuration protocols, it could reflect an attempt to enumerate a device or devices on the same network for further attack.

These alerts are generally provided by network-based intrusion detection systems, configuration server, or the client software.

The appropriate response to these alerts may include:

- Improving the access control of configuration servers and services (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to configuration servers and/or clients
- Removing the configuration service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > CoreAccess

CoreAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources where the related data is mostly or all core protocols (TCP, UDP, IP, ICMP). Generally, CoreAccess alerts reflect attempted exploitation of weaknesses in network protocols or devices with intent to gain access to servers, clients, or network infrastructure devices.

These alerts are generally provided by network-based intrusion detection systems. In some cases, network infrastructure devices such as firewalls or routers may also provide them. In other cases, these events are escalated from the Audit tree through policy.

Events placed in the parent CoreAccess alert are known to be related to a core protocol. However, they are not able to be further categorized based on the message provided by the connector or because they are uncommon.

AttackBehavior > ResourceAttack > NetworkAttack > Access > CoreAccess > ICMPRedirectAccess

ICMPRedirectAccess alerts reflect a specific type of CoreAccess alert where the attack traffic is all ICMP Redirects (ICMP type 5) and the intent is to redirect traffic to enumerate devices or client machines or gather information on devices or client traffic to further attack those or other resources.

Redirects are generally benign ICMP messages sent to hosts to redirect traffic intended for a network that another gateway can control. In cases where ICMP Redirects are used for attacking, a host will generally pretend to be a router, pass a redirect to a client machine to modify its routing table to send traffic to the false router instead of their normal network gateway, and proceed to enumerate, gather information, or attack the redirected host. As a result, the false router will send the traffic on to the correct gateway while the host has no idea of what has occurred (unless another device or connector detects it). This is one type of what is commonly referred to as a man-in-the-middle attack.

These alerts are generally provided by network-based intrusion detection systems and network infrastructure devices, such as firewalls or routers.

The appropriate response to these alerts may include:

- Blocking or resetting the local or remote user's connection/IP address
- Updating the network infrastructure devices
- Restricting incoming/outgoing ICMP redirect requests/responses to reflect inappropriate or abusive access

The appropriate methods to prevent ICMP redirect attacks would include:

- Limiting hosts who can broadcast ICMP Redirects across network devices to correct routers and gateways.
- Limiting ingress and egress ICMP traffic.
- Verifying that clients, servers, and network infrastructure devices are configured with the latest operating system or other networking software. This process helps ensure that other attacks related to ICMP Redirect attacks of this type (such as denial of service attacks) do not occur.

AttackBehavior > ResourceAttack > NetworkAttack > Access > CoreAccess > IPFragmentationAccess

IPFragmentationAccess alerts reflect a specific type of CoreAccess alert where the attack traffic is all IP traffic and the intent is to mask possible malicious or abusive data past an IDS or other detection device by using many IP fragments (usually much larger or smaller than normal fragments).

The network infrastructure devices handling the traffic will reassemble and pass on the traffic correctly. However, an IDS on the network may not be able to detect the malicious traffic, but only the presence of fragments. The attack may be allowed to pass through the network either incoming or outgoing, thereby eliminating one line of defense. Normal IP fragmentation (data that was taken apart because it is too large based on network parameters) should not trigger an IPFragmentationAccess alert.

Fragmentation alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

The appropriate response to these alerts may include:

- Blocking or resetting the local or remote user's connection/IP address
- Applying updates or patches to server and/or client software (especially the IDS)
- Updating the network infrastructure devices
- Restricting incoming/outgoing network requests/responses to reflect inappropriate or abusive access

AttackBehavior > ResourceAttack > NetworkAttack > Access > CoreAccess > IPSourceRouteAccess

IPSourceRouteAccess alerts reflect a specific type of CoreAccess alert where the attack traffic is all IP traffic and the intent is generally to misrepresent the originating address to bypass detection.

IPSourceRouteAccess is a type of IP spoofing where an attacker falsifies network information to convince the destination that the given source is something other than the actual source, directing the destination to return the traffic through an IP Source Route option that traces the traffic to the trusted host and then on to the untrusted attacker. The trusted host receives the traffic from the destination and because of the IP Source Route, it passes the traffic on to the untrusted attacker. The data is not modified, and the attacker has tricked the network into passing the traffic on. Generally, while spoofed, clients will attempt to gather information, perform actual attacks on internal or external devices, or perform denial of service attacks.

These alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

Response to IP spoofing is difficult, as the originating host may be alternating spoofed hostnames or IP addresses to continually circumvent detection. However, response to IP spoofing that uses the IP source route could include removing the ability to pass traffic through routers or gateways that contains an IP Source Route option.

Initial appropriate response to these alerts may include blocking or resetting the local or remote user's connection/IP address, which may prove ineffective or unrealistic. Other responses may include:

- Applying updates or patches to server and/or client software
- Updating network infrastructure devices
- Restricting incoming/outgoing network requests/responses to reflect inappropriate or abusive access

Unfortunately, it may be difficult to derail an attempted attack through IP spoofing, as routing and firewall policies (including disallowing traffic with the IP Source Route option) should prevent further access through spoofed addresses.

AttackBehavior > ResourceAttack > NetworkAttack > Access > CoreAccess > IPSpoofAccess

IPSpoofAccess alerts reflect a specific type of CoreAccess alert where the attack traffic is all IP traffic and the intent is to misrepresent the originating address to either bypass detection or misdirect response to attack activity.

IP Spoofing falsifies network information to convince the destination (and any network hops in between) that the given source is something other than the actual source. Generally, while spoofed, clients will attempt to gather information, perform actual attacks on internal or external devices, or perform denial of service attacks.

These alerts are generally provided by network-based intrusion detection systems and network infrastructure devices, such as firewalls or routers. Response to IP spoofing is difficult, as the originating host may be alternating spoofed hostnames or IP addresses to continually circumvent detection.

Initial appropriate response to these alerts may include blocking or resetting the local or remote user's connection/IP address. However, this may prove ineffective or unrealistic. Other responses may include:

- Applying updates or patches to server and/or client software
- Updating infrastructure devices
- Restricting incoming/outgoing network requests/responses to reflect inappropriate or abusive access.

Unfortunately, it may prove difficult to derail an attempted attack through IP spoofing. Routing and firewall policies should prevent further access through spoofed addresses.

AttackBehavior > ResourceAttack > NetworkAttack > Access > CoreAccess > TCPhijackAccess

TCPhijackAccess alerts reflect a specific type of CoreAccess alert where the attack traffic is all TCP traffic and the intent is to hijack a user's connection.

The intent of TCP Hijacking is to take over another network user's connection by sending malformed packets to confuse the server into thinking that the new user is the original user. In doing so, the original user is removed from his connection to the server and the new user injects himself, taking over all attributes the server assumed from the original, including levels of security and/or trust.

TCP Hijacking can be used to place future attack connectors on client systems, gather information about networks and/or client systems, immediately attack internal networks, or other malicious and/or abusive behavior.

These alerts are generally provided by network-based intrusion detection systems. In some cases, network infrastructure devices (such as firewalls or routers) may also provide them.

The appropriate response to these alerts may include:

- Blocking or resetting the remote hijacker's connection/IP address.
- Applying updates or patches to server and/or client software.
- Applying updates to network infrastructure devices.
- Restricting incoming/outgoing network requests/responses to reflect inappropriate or abusive access.

AttackBehavior > ResourceAttack > NetworkAttack > Access > CoreAccess > TCPTunnelingAccess

TCPTunnelingAccess alerts reflect a specific type of CoreAccess alert where the attack traffic is all TCP traffic and the intent is to tunnel a possible malicious or abusive connection through other TCP traffic.

TCP tunneling uses permitted TCP traffic to bypass access policies on network devices, content filtering, monitoring, and other traffic shaping or behavior policies. TCP tunneling is performed by initiating a known, 'acceptable' TCP connection through allowed policies and piggybacking an unacceptable connection atop the granted one.

On the new 'tunnel' that the user built, they are allowed to pass any traffic through that does not match other policies. Often, after the connection is initiated, it may be difficult to detect and prevent further malicious or abusive activity.

These alerts are generally provided by network-based intrusion detection systems. In some cases, they are provided by network infrastructure devices such as firewalls or routers.

The appropriate response to these alerts may include:

- Blocking or resetting the local or remote user's connection/IP address, applying updates or patches to server and/or client software.
- Updating network infrastructure devices.

- Restricting incoming/outgoing network requests/responses to reflect inappropriate or abusive access.

AttackBehavior > ResourceAttack > NetworkAttack > Access > FileSystemAccess

FileSystemAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through remote file system traffic (using protocols such as SMB and NFS). Generally, these alerts reflect attempted exploitation of weaknesses in the remote file system server, client software, or attempts to gain system-level access to remote file system servers.

These alerts are generally provided by network-based intrusion detection systems, remote file system server, or client software.

The appropriate response to these alerts may include:

- Improving access control of remote file systems (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote file system servers and/or clients
- Removing the remote file system service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > FileSystemAccess > NFSAccess

NFSAccess alerts are a specific type of FileSystemAccess alert that reflects malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through NFS (network file share) remote filesystem traffic. Generally, these alerts reflect attempted exploitation of weaknesses in the NFS server or client software or attempts to gain system-level access to NFS servers themselves.

These alerts are generally provided by network-based intrusion detection systems, the remote file system server, or the client software itself.

The appropriate response to these alerts may include:

- Improving access control of remote file systems (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote file system servers and/or clients.
- Removing the remote file system service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > FileSystemAccess > SMBAccess

SMBAccess alerts are a specific type of FileSystemAccess alert that reflects malicious or abusive usage of network resources where the intention or result is gaining access to resources through server message block (SMB) remote file system traffic. Generally, these alerts reflect attempted exploitation of weaknesses in the SMB server or client software or attempts to gain system-level access to SMB servers.

These alerts are generally provided by network-based intrusion detection systems, remote file system server, or the client software.

The appropriate response to these alerts may include.

- Improving access control of remote file systems (such restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote file system servers and/or clients
- Removing the remote file system service or client application related to this event.

AttackBehavior > ResourceAttack > NetworkAttack > Access > LinkControlAccess

LinkControlAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources where the related data is low-level link control (using protocols such as ARP). Generally, LinkControlAccess alerts reflect attempted exploitation of weaknesses in switching devices by using malformed incoming or outgoing data with the intent to enumerate or gain access to or through switching devices, clients that are also on the switching device, and entire networks attached to the switching device. In some cases, a managed switch with restrictions on port analyzing activity may be forced into an unmanaged switch with no restrictions, allowing a malicious client to sniff traffic and enumerate or attack.

These alerts are generally provided by network-based intrusion detection systems and network infrastructure devices with link level control (such as switches).

The appropriate response to LinkControlAccess events may include:

- Clearing the link-level control mechanisms of the switching device (such as flushing the ARP cache)
- applying updates or patches to switching devices
- Improving segmentation of networks to prevent information disclosure if an attack occurs

AttackBehavior > ResourceAttack > NetworkAttack > Access > PointToPointAccess

PointToPointAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through point-to-point traffic (using protocols such as PPTP). Generally, these alerts will reflect attempted exploitation of weaknesses in point to point server or client software, attempts to enumerate networks, or attempts to further attack devices on trusted networks.

These alerts are generally provided by network-based intrusion detection systems. In some cases, network infrastructure devices such as firewalls, routers, or VPN servers may also provide them.

The appropriate response to these alerts may include:

- Improving access control of remote access services (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote access servers and/or clients
- Removing the remote point to point service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > PointToPointAccess > PPTPSpoof

PPTPSpoof alerts reflect a specific type of PointToPointAccess alert where the attack traffic is all point to point tunneling protocol (PPTP) traffic and the intent is to misrepresent the originating address to either bypass detection or misdirect response to attack activity. Often, the target of these attacks are internal trusted networks that allow remote access through PPTP tunneling.

PPTP spoofing is performed by falsifying network information to convince the destination (and any network hops in between) that the given source is something other than the actual source. Generally, while spoofed, clients attempt to gather information, perform actual attacks on internal devices, or perform denial of service attacks.

These alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers. Response to PPTP spoofing is difficult, as the originating host appears to be coming from a trusted address that completed initial handshaking and key sharing.

The initial appropriate response to these alerts may include:

- Blocking or resetting the local or remote user's connection/IP address
- Applying updates or patches to server and/or client software
- Applying updates to network infrastructure devices
- Restricting incoming/outgoing PPTP traffic requests/responses to reflect inappropriate or abusive access

AttackBehavior > ResourceAttack > NetworkAttack > Access > RemoteProcedureAccess

RemoteProcedureAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through remote procedure call traffic (using protocols such as the traditional RPC services, RMI, and CORBA). Generally, these alerts reflect attempted exploitation of weaknesses in the remote procedure server or client software or attempts to gain system-level access to remote procedure servers.

These alerts are generally provided by network-based intrusion detection systems, the remote procedure server, or the client software.

The appropriate response to these alerts may include:

- Improving access control of remote procedure (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote procedure servers and/or clients
- Removing the remote procedure service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > RemoteProcedureAccess > RPCPortmapperAccess

RPCPortmapperAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through remote procedure call traffic using the traditional RPC portmapper service.

Generally, these alerts reflect attempted exploitation of weaknesses in the remote procedure server or client software or attempts to gain system-level access to remote procedure servers themselves. These alerts are generally provided by network-based intrusion detection systems, the remote procedure server, or the client software.

The appropriate response to these alerts may include:

- Providing improved access control of remote procedure (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to remote procedure servers and/or clients
- Removing the remote procedure service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Access > RoutingAccess

RoutingAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources where the related data is routing-related protocols (RIP, IGMP, and so on). Generally, RoutingAccess alerts reflect attempted exploitation of weaknesses in routing protocols or devices with the intent to enumerate or gain access to or through routers, servers, clients, or other network infrastructure devices. These routing protocols are used to automate the routing process between multiple devices that share or span networks.

These alerts are generally provided by network-based intrusion detection systems and network infrastructure devices that use routing protocols, such as firewalls and routers.

The appropriate response to RoutingAccess events may include:

- Improving access control of the routing devices (such as restriction of what devices are allowed to update routing by IP address to ensure only trusted devices are passing data)
- Applying updates or patches to routing servers and/or devices
- Removing the automated routing protocols from servers and/or devices

AttackBehavior > ResourceAttack > NetworkAttack > Access > RoutingAccess > MalformedRIPAccess

MalformedRIPAccess alerts reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources where the related data is all Routing Information Protocol (RIP).

Generally, MalformedRIPAccess alerts reflect attempted exploitation of weaknesses in RIP by using malformed incoming or outgoing data, with the intent to enumerate or gain access to or through routers, servers, clients, or other network infrastructure devices. RIP automates the routing process between multiple devices that share or span networks.

These alerts are generally provided by network-based intrusion detection systems and network infrastructure devices that use routing protocols such as firewalls and routers.

The appropriate response to RIP Access events may include:

- Improved access control of the routing devices (such as restriction of what devices are allowed to update routing by IP address to ensure only trusted devices are passing data).
- Apply updates or patches to routing servers and/or devices.
- Remove the automated routing protocols from servers and/or devices.

AttackBehavior > ResourceAttack > NetworkAttack > Access > TrojanTrafficAccess

TrojanTrafficAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through malicious code commonly known as a Trojan Horse.

This alert detects the communication related to trojans over the network (generally, trojaned clients calling home to the originator). Trojans are generally executables that generally require no user intervention to spread and contain malicious code that is placed on the client system and used to exploit the client (and return access to the originator of the attack) or exploit other clients (used in attacks such as distributed denial of service attacks).

These alerts are generally provided by a virus scanner, a network-based intrusion detection system, or in some cases, the operating system or network infrastructure devices such as firewalls and routers.

The appropriate response to these alerts may include:

- Quarantine the node from the network to prevent internal attacks and further compromise of the client system.
- Update the virus scanner pattern files on this and other network nodes to prevent future or further infection.

- Perform virus scans on this and other network nodes to detect further infection if any has taken place.
- Research into the offending Trojan to find out methods of removal (if necessary).

AttackBehavior > ResourceAttack > NetworkAttack > Access > TrojanTrafficAccess > TrojanCommandAccess

TrojanCommandAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through malicious code commonly known as Trojan Horses.

This alert detects the communication related to trojans sending commands over the network (infecting other clients, participating in a denial of service activity, being controlled remotely by the originator, and so on). Trojans are generally executables that generally require no user intervention to spread and contain malicious code that is placed on the client system and used to exploit the client (and return access to the originator of the attack) or exploit other clients (used in attacks such as distributed denial of service attacks).

These alerts are generally provided by a virus scanner, a network-based intrusion detection system, or in some cases, the operating system or network infrastructure devices such as firewalls and routers.

The appropriate response to these alerts may include:

- Quarantine the node from the network to prevent internal attacks and further compromise of the client system.
- Update virus scanner pattern files on this and other network nodes to prevent future or further infection.
- Perform virus scans on this and other network nodes to detect further infection if any has taken place.
- Research the offending trojan to find out methods of removal (if necessary).

AttackBehavior > ResourceAttack > NetworkAttack > Access > TrojanTrafficAccess > TrojanInfectionAccess

TrojanInfectionAccess alerts reflect malicious or abusive usage of network resources where the intention or result is gaining access to resources through malicious code commonly known as a Trojan Horse.

This alert detects the infection traffic related to a Trojan entering the network (generally with intent to infect a client). Trojans are generally executables that usually require no user intervention to spread. They contain malicious code that is placed on the client system. This code exploits the client (and return access to the originator of the attack) or exploit other clients (used in attacks such as distributed denial of service attacks).

These alerts are generally provided by a virus scanner, a network-based intrusion detection system, or in some cases, the operating system or network infrastructure devices such as firewalls and routers.

The appropriate response to these alerts may include:

- Quarantine the node from the network to prevent internal attacks and further compromise of the client system
- Update the virus scanner pattern files on this and other network nodes to prevent future or further infection, virus scans on this and other network nodes to detect further infection if any has taken place
- Research the offending trojan to find out methods of removal (if necessary)

AttackBehavior > ResourceAttack > NetworkAttack > Access > VirusTrafficAccess

VirusTrafficAccess alerts reflect malicious or abusive usage of network resources where the intention, or the result, is gaining access to resources through malicious code commonly known as viruses.

This alert detects the communication related to viruses over the network (generally, the spread of a virus infection or an incoming virus infection). Viruses are generally executables that require user intervention to spread, contain malicious code that is placed on the client system, and exploit the client and possibly spread itself to other clients.

These alerts are generally provided by a virus scanner, a network-based intrusion detection system, or in some cases, the operating system or network infrastructure devices such as firewalls and routers.

Appropriate response to these alerts may include:

- Quarantine the node from the network to prevent internal attacks and further compromise of the client system
- Update the virus scanner pattern files on this and other network nodes to prevent future or further infection, virus scans on this and other network nodes to detect further infection if any has taken place
- Research the offending virus to find out methods of removal (if necessary)

AttackBehavior > ResourceAttack > NetworkAttack > Denial

Children of the Denial tree define events centered on malicious or abusive usage of network bandwidth/traffic where the intention or result is inappropriate or abusive access to network resources through a denial of service attack.

These alerts are generally provided by network-based intrusion detection systems, but can also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > ApplicationDenial

ApplicationDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer protocols. The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

ApplicationDenial events may be attempts to exploit weaknesses in software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems. They can also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > ApplicationDenial > FileTransferDenial

FileTransferDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer file transfer-related protocols (FTP, TFTP, etc.). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

FileTransferDenial events may be attempts to exploit weaknesses in file transfer-related software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities. These alerts are generally provided by network-based intrusion detection systems. They can also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > ApplicationDenial > MailDenial

MailDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer mail-related protocols (SMTP, IMAP, POP3, etc.) or services (majordomo, spam filters, etc.). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

MailDenial events can be attempts to exploit weaknesses in mail-related software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems. They may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > ApplicationDenial > MailDenial > MailServiceDenial

MailServiceDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer mail-related services (majordomo, spam filters, and so on). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack. MailServiceDenial events can be attempts to exploit weaknesses in mail-related software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > ApplicationDenial > MailDenial > MailServiceDenial > MailSpamDenial

MailSpamDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer mail-related services (usually SMTP). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack through excessive mail relaying.

MailSpamDenial events reflect excessive attempts to relay mail through an SMTP server from remote sites that should not typically be relaying mail through the server, let alone excessive quantities of mail. The goal of these attacks may not be to enumerate or exploit weaknesses in the mail server, but to relay as much mail through an open relay mail server as quickly as possible, resulting in a denial of service attack.

These alerts are generally provided by network-based intrusion detection systems. They can also be provided by the mail server, firewalls, or other network infrastructure devices. These alerts can indicate an open relay on the network or an attempt to find an open relay. The appropriate response can be to restrict access to SMTP servers to only internal and necessary external IP addresses.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > ApplicationDenial > WebDenial

WebDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is application-layer web-related protocols (HTTP, HTTPS, and so on) or services (CGI, ASP, and so on). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

WebDenial events may be attempts to exploit weaknesses in web-related software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems. They can also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial

CoreDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is core protocols (TCP, IP, ICMP, UDP). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack. CoreDenial events may be attempts to exploit weaknesses in software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems. They can also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > ChargenDenial

ChargenDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service through UDP character generator (chargen) or echo services.

This attack attempts to exploit network infrastructure devices and hosts by pointing two character generator (chargen) or echo hosts at each other. This process forces a multitude of responses, flooding the network and hosts. In response to a request to the echo or character generator (chargen) port, the second device sends a response, which triggers another request, which triggers a response, and so on. The source of the initial request is a spoofed IP address that appears as one of the hosts, which will be a party in the attack (sent to the second host). This will render both devices and possibly the network they are on useless either temporarily or for a significant amount of time by the sheer amount of traffic that is created.

ChargenDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > ICMPFloodDenial

ICMPFloodDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service by an ICMPbased flood attack that uses several, very large ICMP packets.

The network infrastructure devices handling the traffic may pass on the traffic correctly. However, any vulnerable client or device on the network may not be able to process the incoming traffic (it may use up system resources to the point where the device is rendered useless and cannot accept network connections). Normal ICMP Traffic should not trigger an ICMPFloodDenial alert.

ICMPFloodDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > ICMPFragmentationDenial

ICMPFragmentationDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack by using several ICMP fragments (usually either much larger or smaller than normal fragments).

The network infrastructure devices handling the traffic will reassemble and pass on the traffic correctly. However, any vulnerable client on the network may not be able to reassemble the fragmented traffic (it may overflow the stack, triggering a host or service crash). Normal ICMP fragmentation (data that was disassembled because it is too large based on network parameters) should not trigger an ICMPFragmentationDenial alert.

Fragmentation alerts themselves are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > ICMPSourceQuenchDenial

ICMPSourceQuenchDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service by an ICMP-based attack (which uses many ICMP packets set to type 4 - Source Quench).

The network infrastructure devices handling the traffic may pass on the traffic correctly. However, any client listening and responding to source quench traffic may be slowed down to the point where rendered useless by way of correct response to the quench request. Normal ICMP traffic (including single, normal, source quench packets) should not trigger an ICMPSourceQuenchDenial alert.

ICMPSourceQuenchDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > IPFloodDenial

IPFloodDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service by an IP-based flood attack (which uses several, very large IP packets).

The network infrastructure devices handling the traffic may pass on the traffic correctly. However, any vulnerable client or device on the network may not be able to process the incoming traffic (it may use up system resources to the point where the device is rendered useless and cannot accept network connections). Normal IP Traffic should not trigger an IPFloodDenial alert.

IPFloodDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > IPFragmentationDenial

IPFragmentationDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack by using many IP fragments (usually either much larger or smaller than normal fragments).

The network infrastructure devices handling the traffic will reassemble and pass on the traffic correctly. However, any vulnerable client on the network may not be able to reassemble the fragmented traffic (it may overflow the stack, triggering a host or service crash). Normal IP fragmentation (data that was taken apart because it is too large based on network parameters) should not trigger an IPFragmentationDenial alert.

Fragmentation alerts themselves are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > IPFragmentationDenial > PingOfDeathDenial

PingOfDeathDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service by a 'ping of death' attack (which uses many large ICMP Echo Request packets).

The network infrastructure devices handling the traffic will pass on the traffic correctly. However, any vulnerable client on the network may not be able to process the incoming traffic (it may be processed in such a way that triggers a host or service crash). Unpatched Windows NT and 95/98 clients are especially vulnerable to this type of attack.

Normal ICMP Echo Traffic should not trigger a PingOfDeathDenial alert. PingOfDeathDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > LandAttackDenial

LandAttackDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service by a land attack. This type of attack uses TCP traffic with the SYN bit set and the same source IP and port as the destination.

The network infrastructure devices handling the traffic will pass on the traffic correctly. However, any vulnerable client on the network may not be able to process the incoming traffic (it may be processed in such a way that triggers a host or service crash). Normal TCP traffic (with or without the SYN bit) should not trigger a LandAttackDenial alert.

LandAttackDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > SmurfDenial

SmurfDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service by a 'Smurf' attack.

A Smurf attack attempts to exploit a vulnerability in some network infrastructure devices by sending ICMP Echo Requests to devices that will re-broadcast the traffic to internal devices. In response to the broadcast Echo Request, all of the devices will send an ICMP Echo Reply, which will effectively overflow the device.

The destination of the ICMP Echo Reply is a spoofed 'victim' IP address that will also be overflowed by the actual replies sent to their host. This will render both devices useless either temporarily or for a significant amount of time.

SmurfDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > SnorkDenial

SnorkDenial alerts reflect a specific type of CoreDenial alert where the intent, or the result, of this activity is inappropriate or abusive access to network resources through a denial of service by a 'Snork' attack.

A Snork attack attempts to exploit a vulnerability in Windows NT devices by using the Windows RPC service and sending packets to devices that will broadcast the traffic to other internal Windows NT devices using RPC. In response to the broadcast, all of the Windows NT devices will send another packet, and this process will continue until it effectively overflows the device and possibly the network.

The destination or source of the initial packet is a spoofed 'victim' IP address which will create the illusion of internal activity. This will render both devices useless either temporarily or for a significant amount of time.

SnorkDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > SynFloodDenial

SYNFloodDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service by a TCP-based 'flood' attack. This attack uses several, very large TCP packets with the SYN bit set.

The network infrastructure devices handling the traffic may pass on the traffic correctly. However, any vulnerable client or device on the network may not be able to process the incoming traffic. It may use up system resources to the point where the device is rendered useless and cannot accept network connections. Normal TCP Traffic (with or without the SYN flag) should not trigger a SYNFloodDenial alert.

SYNFloodDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > TeardropDenial

TeardropDenial alerts reflect a specific type of CoreDenial alert where the intent or result of this activity is inappropriate or abusive access to network resources through a denial of service by a teardrop attack. This type of attack uses many overlapping IP fragments, usually either much larger or smaller than normal fragments.

The network infrastructure devices handling the traffic will reassemble and pass on the traffic correctly. However, any vulnerable client on the network may not be able to reassemble the fragmented traffic. The traffic may be reassembled in such a way that triggers a host or service crash. Normal IP fragmentation (data that was disassembled because it is too large based on network parameters) should not trigger a TeardropDenial alert.

TeardropDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > CoreDenial > UDPBombDenial

UDPBombDenial alerts reflect a specific type of CoreDenial alert where the intent or result, of this activity is inappropriate or abusive access to network resources through a denial of service by a UDP-based 'bomb' attack. This type of attack uses several large UDP packets.

The network infrastructure devices handling the traffic may pass on the traffic correctly. However, any vulnerable client or device on the network may not be able to process the incoming traffic. It may be processed in such a way that triggers a host or service crash. Normal UDP Traffic should not trigger a UDPBombDenial alert.

UDPBombDenial alerts are generally provided by network-based intrusion detection systems and network infrastructure devices such as firewalls or routers.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > ConfigurationDenial

ConfigurationDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is protocols related to configuration of resources (DHCP, BootP, SNMP, etc.). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

ConfigurationDenial events may be attempts to exploit weaknesses in configuration-related software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > FileSystemDenial

FileSystemDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is remote file system-related protocols (NFS, SMB, and so on). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

FileSystemDenial events may be attempts to exploit weaknesses in remote file system services or software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > LinkControlDenial

LinkControlDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is link level protocols (such as ARP). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

LinkControlDenial events may be attempts to exploit weaknesses in link-level control software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > RemoteProcedureDenial

RemoteProcedureDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is remote procedure-related protocols (traditional RPC, RMI, CORBA, etc.) or service (portmapper, etc.). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

RemoteProcedureDenial events may be attempts to exploit weaknesses in remote procedure services or software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > RemoteProcedureDenial > RPCPortmapperDenial

RPCPortmapperDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is remote procedure-related protocols specifically related to the RPC portmapper service. The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

RPCPortmapperDenial events may be attempts to exploit weaknesses the remote procedure service or software to gain access to a host system, attempts to exploit weaknesses in the software to enumerate or reconfigure, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > RoutingDenial

RoutingDenial events are a specific type of Denial event where the transport of the malicious or abusive usage is routing-related protocols (RIP, IGMP, etc.). The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

RoutingDenial events may be attempts to exploit weaknesses in routers or routing software to gain access to a host system, attempts to exploit weaknesses in the routing software or service to enumerate or reconfigure, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Denial > TrojanTrafficDenial

TrojanTrafficDenial events are a specific type of Denial event where the transport of the malicious or abusive usage originates with malicious code on a client system known as a Trojan. The intent or result of this activity is inappropriate or abusive access to network resources through a denial of service attack.

TrojanTrafficDenial events may be attempts to exploit weaknesses in software to gain access to a host system, attempts to exploit weaknesses in network infrastructure equipment to enumerate or reconfigure devices, attempts to spread the Trojan to other hosts, or other denial of service activities.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Relay

Children of the Relay tree define events centered on malicious or abusive usage of network bandwidth/traffic where the intent or result is relaying inappropriate or abusive access to other network resources (either internal or external).

Generally, these attacks will have the perimeter or an internal host as their point of origin. When sourced from remote hosts, they may indicate a successful exploit of an internal or perimeter host.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

AttackBehavior > ResourceAttack > NetworkAttack > Relay > DDOSToolRelay

DDOSToolRelay events reflect potential network traffic related to known Distributed Denial of Service connectors. These connectors are used to relay attacks to new remote (and possibly local) hosts to exploit or inundate the remote host with data in an attempt to cripple it.

Generally, these attacks will have a perimeter or an internal host as their point of origin. When sourced from remote hosts, they may indicate a successful exploit of an internal or perimeter host.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by firewalls or other network infrastructure devices.

The appropriate response to these events may include:

- Restrict the source from accessing any external network
- Run a virus scanner or other detection utility to detect and remove the presence of any relay connector (in some cases known as a 'zombie')
- Quarantine the source node from the network to further isolate the issue (if necessary)

If these events are sourced from a completely external network, the appropriate actions may include:

- Blocking the remote host
- Provide better access control of clients, servers, and services, such as restriction by IP address and/or user name to ensure only trusted clients can connect
- Apply updates or patches to servers and/or clients
- Remove the service related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Relay > FileTransferRelay

FileTransferRelay events reflect potential network traffic related to known attack connectors that operate over file transfer protocols. These connectors are used to relay attacks to new remote (and possibly local) hosts to exploit or abuse services.

Generally, these attacks will have a perimeter or an internal host as their point of origin. When sourced from remote hosts, they may indicate a successful exploit of an internal or perimeter host.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by the file transfer software itself, and firewalls or other network infrastructure devices.

The appropriate response to these events may include:

- Restrict the source from accessing any external network
- Run a virus scanner or other detection utility to detect and remove the presence of any relay connector
- Quarantine the source node from the network to further isolate the issue (if necessary)

If these events are sourced from a completely external network, the appropriate actions may include:

- Blocking the remote host, better access control of file transfer servers (such as restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to file transfer servers and/or clients
- Removing the file transfer service or client application related to this event

AttackBehavior > ResourceAttack > NetworkAttack > Relay > FileTransferRelay > FTPBounce

FTPBounce events are a specific type of FileTransferRelay related to known attack connectors using file transfer protocols that are used to launder connections to other services, redirect attacks to other hosts or services, or to redirect connections to other hosts or services.

Generally, these attacks will have a perimeter or an internal host as their point of origin. When sourced from remote hosts, they may indicate a successful exploit of an internal or perimeter host.

These alerts are generally provided by network-based intrusion detection systems, but may also be provided by the file transfer software or service itself, and firewalls or other network infrastructure devices.

The appropriate response to these events may include:

- Restrict the source from accessing any external network
- Run a virus scanner or other detection utility to detect and remove the presence of any relay connector
- Quarantine the source node from the network to further isolate the issue (if necessary)

If these events are sourced from a completely external network, the appropriate actions may include:

- Blocking the remote host
- Providing better access control of file transfer servers (such restriction by IP address and/or user name to ensure only trusted clients are connecting)
- Applying updates or patches to file transfer servers and/or clients
- Removing the file transfer service or client application related to this event

AttackBehavior > ResourceAttack > ServiceProcessAttack

Members of the ServiceProcessAttack tree define events centered on malicious or abusive usage of services or user processes. These events include abuse or misuse of resources from malicious code placed on the client system.

AttackBehavior > ResourceAttack > ServiceProcessAttack > VirusAttack

VirusAttack alerts reflect malicious code placed on a client or server system, which may lead to system or other resource compromise and further attack. The severity of this alert depends on the ActionTaken field, which reflects whether the virus or other malicious code was successfully removed.

These alerts are usually provided by a virus scanner running on the client system. The appropriate response to these alerts may include:

- Quarantine the node from the network to prevent further outbreak
- Update the virus scanner pattern files on other network nodes to prevent further outbreak
- Run virus scans on other network nodes to detect further outbreak if any has taken place
- Research the offending virus to discover removal methods

AttackBehavior > ResourceAttack > ServiceProcessAttack > VirusSummaryAttack

VirusSummaryAttack alerts reflect malicious code placed on a client or server system, which may lead to system or other resource compromise and further attack. The severity of this alert depends on the ActionTaken field that reflects whether the virus or other malicious code was successfully removed. These alerts differ from VirusAttack in that they may be a composite of virus events normally due to a scheduled scan on the client system as opposed to a real-time scan.

These alerts are usually provided by a virus scanner running on the client system. Appropriate response to these alerts may include:

- Quarantine the node from the network to prevent further outbreak
- Update the virus scanner pattern files on other network nodes to prevent further outbreak
- Run virus scans on other network nodes to detect further outbreak if any has taken place
- Research into the offending virus to discover removal methods

GeneralSecurity

GeneralSecurity alerts are generated when a supported product outputs data is not normalized into a specific alert, but is known to be a security-related issue.

SuspiciousBehavior

Events that are children of SuspiciousBehavior are generally related to network activity that may be consistent of:

- Enumeration of resources
- Unexpected traffic
- Abnormal authentication events
- Other abnormal behavior that should be considered indicative of a serious security event

SuspiciousBehavior > AuthSuspicious

Members of the AuthSuspicious tree define events regarding suspicious authentication and authorization events. These events include:

- Excessive failed authentication or authorization attempts
- Suspicious access to unauthenticated users
- Suspicious access to unauthorized services or information

SuspiciousBehavior > AuthSuspicious > FailedAuthentication

FailedAuthentication events occur when a user makes several attempts to authenticate themselves and continuously fails, or when a logon failure is serious enough to merit a security event on a single failure.

SuspiciousBehavior > AuthSuspicious > GuestLogin

GuestLogin events describe user authentication events where a successful or unsuccessful attempt was made to grant access to a user that generally has no assigned password (such as anonymous, guest, or default) and no special privileges. A user with this privilege level may be granted access to enough of the client system to begin exploitation.

These events are usually produced by a client or server operating system. However, they may also be produced by a network-based IDS or network infrastructure device when it is possible or appropriate.

SuspiciousBehavior > AuthSuspicious > RestrictedInformationAttempt

RestrictedInformationAttempt events describe a user attempt to access local or remote information that their level of authorization does not allow. These events may indicate user attempts to exploit services that they are denied to or inappropriate access attempts to restricted information.

SuspiciousBehavior > AuthSuspicious > RestrictedServiceAttempt

RestrictedServiceAttempt events describe a user attempt to access a local or remote service that their level of authorization does not allow. These events may indicate user attempts to exploit services that they are denied access to or inappropriate access attempts to services.

SuspiciousBehavior > InferredSuspicious

InferredSuspicious alerts are reserved SuspiciousBehavior alerts used to describe suspicious behavior that is a composite of different types of alerts. These events are defined and inferred by policy.

SuspiciousBehavior > ResourceSuspicious

Members of the ResourceSuspicious tree define different types of suspicious access to network resources. These resources may include network bandwidth/traffic, files, client processes or services, or other types of shared security-related commodities.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious

Members of the NetworkSuspicious tree define events regarding suspicious usage of network bandwidth/traffic. These events include unusual traffic and reconnaissance behavior detected on network resources.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon

Children of the Recon tree reflect suspicious network behavior with the intent of gathering information about target clients, networks, or hosts.

Reconnaissance behavior may be valid behavior on a network. However, only as a controlled behavior in small quantities. Invalid reconnaissance behavior can reflect attempts to determine security flaws on remote hosts, missing access control policies that allow external hosts to penetrate networks, or other suspicious behavior that results in general information gathering without actively attacking.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate

Enumerate alerts reflect attempts to gather information about target networks (or specific target hosts) by sending active data that elicit responses and reveal information about clients, servers, or other network infrastructure devices. The originating enumeration source is generally attempting to acquire information that may reveal more than what is revealed by normal traffic to the target.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > ApplicationEnumerate

ApplicationEnumerate alerts reflect attempts to gather information about target hosts, or services on target hosts, by sending active application-layer data which will elicit responses that reveal information about the application or host. This enumeration may be a LEMple command sent to the application to attempt to fingerprint what is allowed or denied by the service, requests to the application which may enable an attacker to surmise the version and specific application running, and other information gathering tactics.

These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the host or application that may work correctly the first time. This process enables them to modify their methodology to continue relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > ApplicationEnumerate > FileTransferEnumerate

FileTransferEnumerate alerts reflect attempts to gather information about target hosts, or services on target hosts, by sending active application-layer data to file transfer services that elicit responses and reveal information about the application or host.

This enumeration may be a simple command sent to the file transfer service to attempt to fingerprint what is allowed or denied by the service, requests to the file transfer service that may enable an attacker to surmise the version and specific service running, and other information gathering tactics.

These enumerations may result in providing information that allows an attacker to craft a specific attack against the file transfer service or application that may work correctly the first time. This enables them to modify their methodology to continue relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > ApplicationEnumerate > FileTransferEnumerate > FTPCommandEnumerate

FTPCommandEnumerate alerts reflect attempts to gather information about target hosts (or services on target hosts) by sending active application-layer data to file transfer services that elicit responses and reveal information about the application.

This enumeration specifically includes commands sent to the FTP service to attempt to fingerprint what is allowed or denied by the service, requests to the FTP service that may enable an attacker to surmise the version and specific service running, and other information gathering tactics that use FTP commands to query. These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the FTP service that may work correctly the first time, enabling them to modify their methodology to continue relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > ApplicationEnumerate > MailEnumerate

MailEnumerate alerts reflect attempts to gather information about target hosts (or services on target hosts) by sending active application-layer data to mail-related services that will elicit responses and reveal information about the application or host.

This enumeration may be a simple command sent to the mail service to attempt to fingerprint what is allowed or denied by the service, requests to the mail service that may enable an attacker to surmise the version and specific service running, and other information gathering tactics. These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the mail service or application that may work correctly the first time - enabling them to modify their methodology to go on relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > ApplicationEnumerate > MailEnumerate > SMTPCommandEnumerate

SMTPCommandEnumerate alerts reflect attempts to gather information about target hosts, or services on target hosts, by sending active application-layer data to mail-related services that will elicit responses and reveal information about the application.

This enumeration specifically entails commands sent to the SMTP service to attempt to fingerprint what is allowed or denied by the service, requests to the mail service that may enable an attacker to surmise the version and specific service running, and other information gathering tactics that use SMTP commands to query. These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the mail service that may work correctly the first time - enabling them to modify their methodology to go on relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > ApplicationEnumerate > WebEnumerate

WebEnumerate alerts reflect attempts to gather information about target hosts (or services on target hosts) by sending active application-layer data to web-related services that will elicit responses and reveal information about the application or host.

This enumeration may be a simple command sent to the web service to attempt to fingerprint what is allowed or denied by the service, requests to the web service that may enable an attacker to surmise the version and specific service running, and other information gathering tactics. These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the web service or application that may work correctly the first time, enabling them to modify their methodology to go on relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > BannerGrabbingEnumerate

BannerGrabbingEnumerate alerts reflect attempts to gather information about target hosts (or services on target hosts) by sending a request that will elicit a response containing the host or service's 'banner'.

This 'banner' contains information that may provide a potential attacker with details such as the exact application and version running behind a port. These details could be used to craft specific attacks against hosts or services that an attacker may know will work correctly the first time, enabling them to modify their methodology go on relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > MSNetworkingEnumerate

MSNetworkingEnumerate alerts reflect attempts to gather information about target hosts, or services on target hosts, by sending active data to Microsoft networking services (using protocols such as NetBIOS and SMB/CIFS) that will illicit responses that reveal information about the application, host, or target network.

This enumeration may be a simple command sent to the networking service to attempt to fingerprint what is allowed or denied by a service, requests to a service that may enable an attacker to surmise the version and specific service running, requests to a service that may enable an attacker to fingerprint the target network, and other information gathering tactics.

These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the networking service, host, or application that may work correctly the first time, enabling them to modify their methodology to go on relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > RemoteProcedureEnumerate

RemoteProcedureEnumerate alerts reflect attempts to gather information about target hosts (or services on target hosts) by sending active data to Remote Procedure services (using protocols such as RMI, CORBA, and traditional RPC) that elicit responses and reveal information about the application or host.

This enumeration may be a simple command sent to the remote procedure service to attempt to fingerprint what is allowed or denied by the service, requests to the remote procedure service that may enable an attacker to surmise the version and specific service running, and other information gathering tactics.

These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the remote procedure service or application that may work correctly the first time - enabling them to modify their methodology to go on relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > RemoteProcedureEnumerate > RPCPortmapperEnumerate

RPCPortmapperEnumerate alerts reflect attempts to gather information about target hosts, or services on target hosts, by sending active data to the Portmapper Remote Procedure service that will illicit responses that reveal information about the application or host.

This enumeration may be a simple command sent to the portmapper service to attempt to fingerprint what is allowed or denied by the service, requests to the portmapper service that may enable an attacker to surmise the version and specific service running, and other information gathering tactics.

These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the portmapper service or client application that may work correctly the first time, enabling them to modify their methodology to go on relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Enumerate > RemoteProcedureEnumerate > RPCPortScanEnumerate

RPCPortScanEnumerate alerts reflect attempts to gather information about target hosts (or services on target hosts) by sending active data to Remote Procedure services (using protocols such as RMI, CORBA, and traditional RPC) that will elicit responses that reveal information about the application or host.

This specific type of enumeration is performed by sending queries to RPC related ports to attempt to fingerprint the types and specific services running, and may involve other information gathering tactics.

These enumerations may result in information being provided that can allow an attacker to craft a specific attack against the remote procedure service or application that may work correctly the first time - enabling them to modify their methodology to go on relatively undetected.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Footprint

Footprint alerts reflect attempts to gather information about target networks by tracing the network through routers, clients, servers, or other network infrastructure devices. The originating source of the footprint is generally attempting to acquire information that may reveal more about network behavior than normal traffic to the target would.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Footprint > DNSRequestFootprint

DNSRequestFootprint alerts are a specific type of Footprint alert that reflects a DNS record request that may serve to reveal the DNS configuration. Contained within this DNS configuration may be information that reveals internal networks, protected devices, or IP addresses of potential targets.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Footprint > FirewalkingFootprint

FirewalkingFootprint alerts are a specific type of Footprint alert that reflects the usage of a connector that attempts to gather information about network infrastructure device access control and filtering lists.

Firewalking works by passing TCP and UDP packets to determine what packets a given device will forward. This activity may reflect attempts to enumerate devices beyond the perimeter of a network, gathering information about activity that is allowed or denied past given gateways.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Footprint > TraceRouteFootprint

TraceRouteFootprint alerts are a specific type of Footprint alert that reflects an IP packet route trace from source to destination. Generally, this route will not reveal specific information about device types or hosts on a network, but will trace the path of IP traffic across routing devices. This traffic may be an attempt to discover routing devices that are misconfigured (which may be vulnerable to attacks such as IP spoofing or IP fragmentation).

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan

Scan alerts reflect attempts to gather information about target networks (or specific target hosts) by sending scans that will elicit responses and reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include a list of applications listening on ports, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan

CoreScan alerts reflect attempts to gather information about target networks (or specific target hosts) by sending scans over core network protocols (TCP, IP, ICMP, UDP) that will elicit responses and reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include a list of applications listening on ports, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > HostScan

HostScan alerts reflect attempts to gather information about specific target hosts by sending scans which will elicit responses that reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include a list of applications on the host, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

These scans generally do not occur across entire networks and generally have the intent of discovering operating system and application information which may be used for further attack preparation.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > ICMPQuery

ICMPQuery alerts reflect attempts to gather information about specific target hosts (or networks) by sending ICMP-based queries that will elicit responses and reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include operating system information and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

These scans generally do not occur across entire networks, contain many sequential ICMP packets, and generally have the intent of discovering operating system and application information which may be used for further attack preparation.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > PingSweep

PingSweep alerts reflect a specific type of CoreScan alert that describe an attempt to gather information about target networks, and hosts on those networks, by sending ICMP or TCP ping packets to test whether hosts are alive.

The originating source of the scan is generally attempting to acquire information about network topology or groups of specific hosts on the network, and may have the intent of gathering information for future attack attempts.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > PingSweep > ICMPPingSweep

ICMPPingSweep alerts reflect a specific type of CoreScan alert that describe an attempt to gather information about target networks, and hosts on those networks, by sending ICMP ping packets to test whether hosts are alive.

The originating source of the scan is generally attempting to acquire information about network topology or groups of specific hosts on the network, and may have the intent of gathering information for future attack attempts.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > PingSweep > TCPPingSweep

TCPPingSweep alerts reflect a specific type of CoreScan alert that describe an attempt to gather information about target networks, and hosts on those networks, by sending TCP ping packets to test whether hosts are alive.

The originating source of the scan is generally attempting to acquire information about network topology or groups of specific hosts on the network and may have the intent of gathering information for future attack attempts.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > PortScan

PortScan alerts reflect attempts to gather information about target networks, or specific target hosts, by sending scans over core network protocols (TCP, IP, ICMP, UDP) that will elicit responses that reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include a list of applications listening on ports, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

Portscans specifically operate by sending probes to every port within a range, attempting to identify open ports that may use applications or services that are easy to enumerate and attack.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > PortScan > TCPPortScan

TCPPortScan alerts reflect attempts to gather information about target networks (or specific target hosts) by sending scans over TCP that will elicit responses and reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target would. This information can include a list of applications listening on ports, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts. TCP portscans specifically operate by sending TCP probes to every port within a range, attempting to identify open ports that may use applications or services that are easy to enumerate and attack.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > PortScan > UDPPortScan

UDPPortScan alerts reflect attempts to gather information about target networks (or specific target hosts) by sending scans over UDP that will elicit responses and reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include a list of applications listening on ports, operating system information, and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

UDP portscans specifically operate by sending UDP probes to every port within a range, attempting to identify open ports that may use applications or services that are easy to enumerate and attack.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > StackFingerprint

StackFingerprint alerts reflect attempts to gather information about specific target hosts by sending a certain set of packets to probe a device's network stack that will elicit responses and reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include operating system information (including type and version) and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

These scans generally do not occur across entire networks and generally have the intent of discovering operating system information, which may be used for further attack preparation.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > StackFingerprint > ICMPStackFingerprint

ICMPStackFingerprint alerts reflect attempts to gather information about specific target hosts by sending a certain set of ICMP packets to probe a device's ICMP stack that elicit responses and reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include operating system information (including type and version) and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

These scans generally do not occur across entire networks and generally have the intent of discovering operating system information, which may be used for further attack preparation.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > CoreScan > StackFingerprint > TCPStackFingerprint

TCPStackFingerprint alerts reflect attempts to gather information about specific target hosts by sending a certain set of TCP packets to probe a device's TCP/IP stack that elicit responses and reveal information about clients, servers, or other network infrastructure devices.

The originating source of the scan is generally attempting to acquire information that may reveal more than normal traffic to the target. This information can include operating system information (including type and version) and other information that a probe may discover without enumeration of the specific services or performing attack attempts.

These scans generally do not occur across entire networks and generally have the intent of discovering operating system information, which may be used for further attack preparation.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > Recon > Scan > TrojanScanner

TrojanScanner alerts reflect attempts of Trojans on the network to gather information about target networks (or specific target hosts) by sending scans that elicit responses and reveal information about the host.

The originating Trojan source of the scan is generally attempting to acquire information that reveals whether a target host or network has open and available services for further exploitation, whether the target host or network is alive, and how much of the target network is visible. A Trojan may run a scan before attempting an attack operation to test potential effectiveness or targeting information.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > UnusualTraffic

UnusualTraffic alerts reflect suspicious behavior on network devices where the traffic may have no known exploit, but is unusual and could be potential enumerations, probes, fingerprints, attempts to confuse devices, or other abnormal traffic.

UnusualTraffic may have no impending response. However, it could reflect a suspicious host that should be monitored closely.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > UnusualTraffic > UnusualICMPTraffic

UnusualICMPTraffic alerts reflect ICMP-based suspicious behavior on network devices where the traffic may have no known exploit, but is unusual and could be potential enumerations, probes, fingerprints, attempts to confuse devices, or other abnormal traffic.

UnusualICMPTraffic may have no impending response. However, it could reflect a suspicious host that should be monitored closely.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > UnusualTraffic > UnusualIPTraffic

UnusualIPTraffic alerts reflect IP-based suspicious behavior on network devices where the traffic may have no known exploit, but is unusual and could be potential enumerations, probes, fingerprints, attempts to confuse devices, or other abnormal traffic.

UnusualIPTraffic may have no impending response, however, it could reflect a suspicious host that should be monitored closely.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > UnusualTraffic > UnusualProtocol

UnusualProtocol alerts reflect suspicious behavior on network devices where the traffic is targeted at unknown, unassigned, or uncommonly used protocols. This traffic may have no known exploit, but is unusual and should be considered potential enumerations, probes, fingerprints, attempts to confuse devices, or other abnormal traffic.

UnusualProtocol may have no impending response. However, it could reflect a suspicious host that should be monitored closely.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > UnusualTraffic > UnusualTCPTraffic

UnusualTCPTraffic alerts reflect TCP-based suspicious behavior on network devices where the traffic may have no known exploit, but is unusual and could be potential enumerations, probes, fingerprints, attempts to confuse devices, or other abnormal traffic.

UnusualTCPTraffic may have no impending response. However, it could reflect a suspicious host that should be monitored closely.

SuspiciousBehavior > ResourceSuspicious > NetworkSuspicious > UnusualTraffic > UnusualUDPTraffic

UnusualUDPTraffic alerts reflect UDP-based suspicious behavior on network devices where the traffic may have no known exploit, but is unusual and could be potential enumerations, probes, fingerprints, attempts to confuse devices, or other abnormal traffic.

UnusualUDPTraffic may have no impending response. However, it could reflect a suspicious host that should be monitored closely.

Create rules that respond to security events

SEM rules monitor event traffic and automatically respond to security events in real time, whether you are monitoring the console or not.

When an event (or a series of events) meets a rule condition (or set of conditions), the rule prompts the SEM Manager to act. A response action can be discreet (for example, sending a notification to select users by email), or active (for example, blocking an IP address or stopping a process). Learn more about SEM rules [here](#).

 See [About SEM response actions](#) for information about response actions.

Get started building custom rule expressions in SEM

You can [create a custom rule](#) to trigger certain actions when a defined event or events occur. Custom rules can be as simple or as complex as required to meet specific needs. These needs can range from a single yes/no event to a combination of precisely defined occurrences over a period of time. They can trigger actions from sending an email to logging off a user or shutting down a device.

Use discretion when creating rules. SolarWinds recommends that you practice creating filters before you start creating rules. Creating rules is similar to creating filters. Filters report event occurrences, whereas rules act on them.

 Begin configuring rules when you are comfortable with configuring filters. Always test your rules before you implement them in your deployment.

You can create rules by configuring conditions between alert variables and other components (such as time of day sets, user-defined groups, constants, and so on). Using rules, you can correlate alert variables with other alerts and their alert variables.

You can configure rules to fire after multiple alerts occur. SEM remembers alerts that meet the basic rule conditions and waits for additional conditions to be met. The rule does not execute until the alerts meet all the conditions and correlations defined for the rule.

You can specify how often and in what time frame the correlations must be met before the rule is triggered. The combined correlations dictate when the rule initiates an active response.

About SEM rules

Rules respond to one or more events. In many cases, you can base rules on several events that SEM correlates to trigger an action. You can also configure a rule to be triggered by a single event.

 Rules can only fire on normalized data and not on raw log data that is received.

Rules play a key role in detecting operational and compliance issues on your network, such as external breaches, insider abuse, and policy violations. SEM includes a set of preconfigured rules to help you get started.

SEM rule scenarios

Several scenarios can warrant a rule. Consider the following combinations of rules and actions:

- Respond to change management events with the Send Email Message action.
- Respond to port scanning events with the Block IP action.
- Respond to isolated spikes in network traffic with the Send Email Message or Disable Networking action.
- Respond to users playing games on monitored computers with the Send Popup Message or Kill Process action.
- Respond to users attaching unauthorized USB devices to monitored computers using the Detach USB Device action.

 Any activity or event that can pose a threat to your network warrants a SEM rule.

Rule configuration requirements and best practices

Review the following requirements and best practices about creating SEM rules.

Use descriptive rule names

To keep rules simple to manage, SolarWinds recommends creating the rule with a name that describes the event, and a full description.

Set the Correlation, Correlation time, and Action

Each rule requires you to define three settings: Correlation, correlation time, and action.

Correlation is the number of events that occur within a selected amount of time and the amount of time allocated to responding to the events.

Correlation time is the volume of events that match the correlation conditions and the rolling time window to evaluate the correlation.

Action is the action that occurs when the rule is triggered.

Enable a rule to upload local changes

When you create a new rule or change an existing rule, you are working on a local copy of the rule. The SEM Manager cannot use the changed rule until you activate it. Activating a rule tells the SEM Manager to reload its enabled rules and upload updates from your local copies.

Enable rules whenever you create a new rule, edit an existing rule, or change the test mode status. Otherwise, the SEM Manager will not recognize your changes. After enabling rules, SEM begins processing rules.

Verify that a rule fired

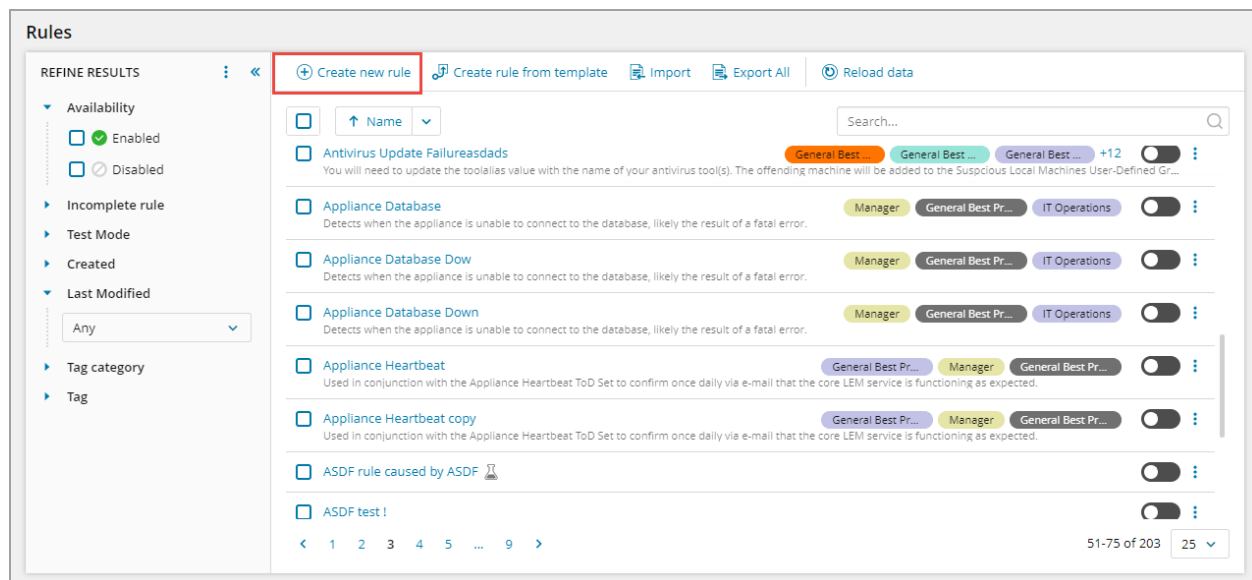
Check your console for `InternalRuleFired` events using a filter. These events will show the triggered rule and when it occurred.

Test new rules before putting them into production

Before you put a rule into production, try it out in [test mode](#). In test mode, the SEM Manager processes the rule alert messages, but does not execute any rule actions. This lets you see how the activated rule will behave without disrupting your network.

Create a new rule

1. Log in to the SEM Console.
2. On the toolbar, click the Rules tab.
3. On the Rules toolbar, click Create new rule.

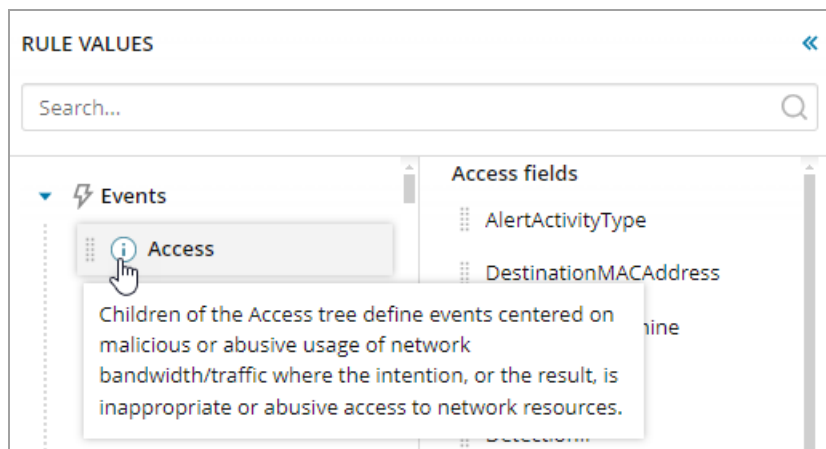


The Create new rule screen displays in the console. The left column displays several categories you can add to a rule, including:

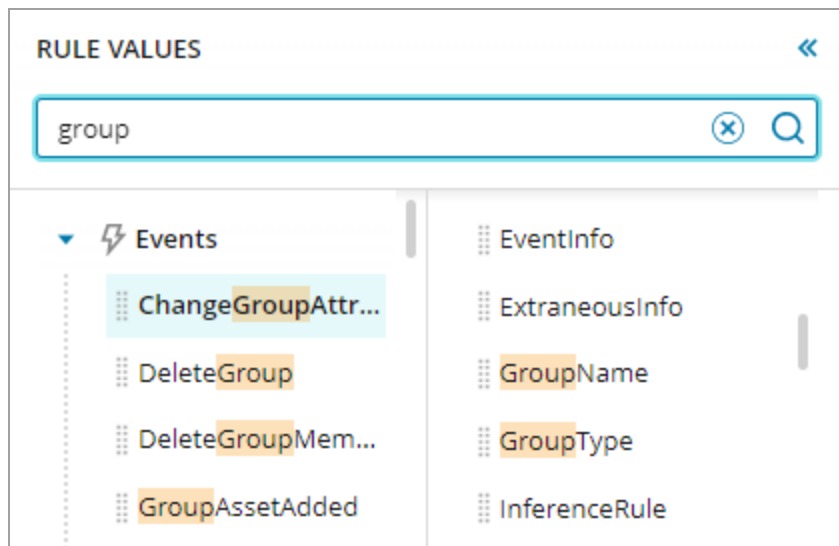
- [Events](#)
- [Event Groups](#)
- [User Defined Groups](#)
- [Directory Service Groups](#)
- [Time Groups](#) (also known as Time of Day Groups)
- [Connector Profiles](#)
- Constants (such as boolean, date, number, and string)

4. Click a category drop-down menu and select an entity for the rule.

All Events entities listed in the left column include predefined contextual help. Click the information  icon to view a description.

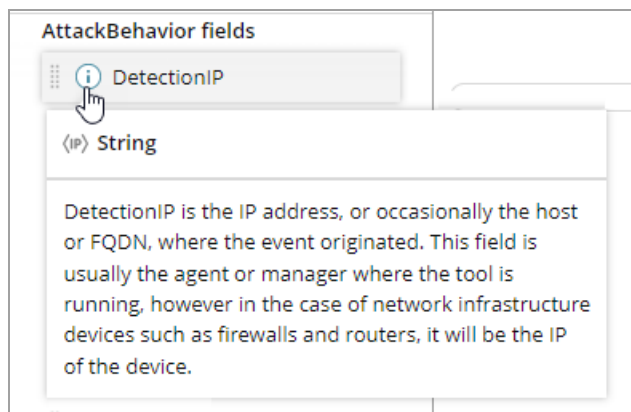


If you are not sure which entity to select, enter a search term in the Search field locate an entity and a corresponding field. All matches are highlighted in the events and field columns.



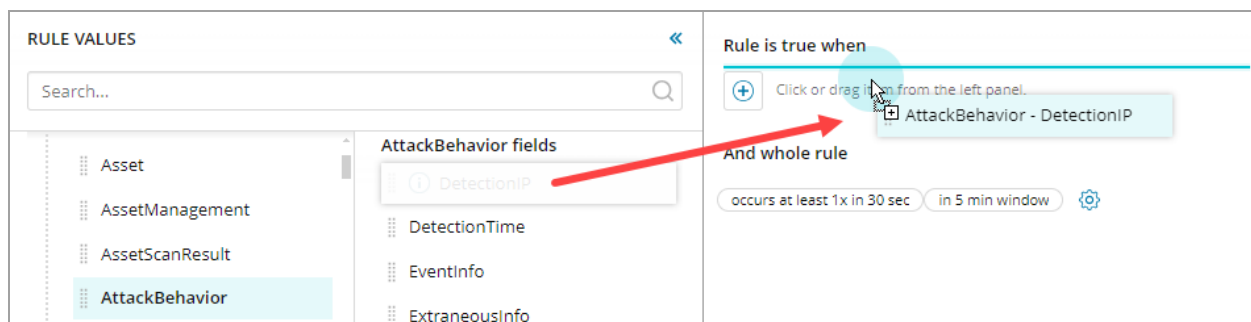
5. Select a corresponding field for the entity (if desired).

All event fields listed in the right column include predefined contextual help. Click the information  icon to view a description.



6. Drag the appropriate entity or entity field into the rule definition builder.

 When you drag an entity or entity field into the rule builder, the correct drop location is shown with a blue line.



Dragging an entity or entity field to the right pane creates a condition. If it is an entity, by default the condition will be created showing that it occurred. For example:

Rule is true when

 Access occurred

If required, click **occurred** to change the value to **did not occur**. If it is an entity field, by default the condition is created, showing that the field is equal to [blank].

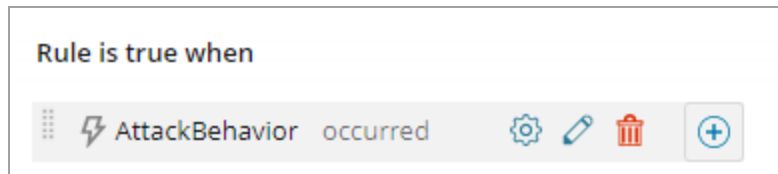
Rule is true when

 AttackBehavior.DetectionIP is equal to

Drop item here, or add it

Click **is equal to** to change to an alternative operator as required. Enter a value for the comparison, click to display the available value, or drag across another field as appropriate.

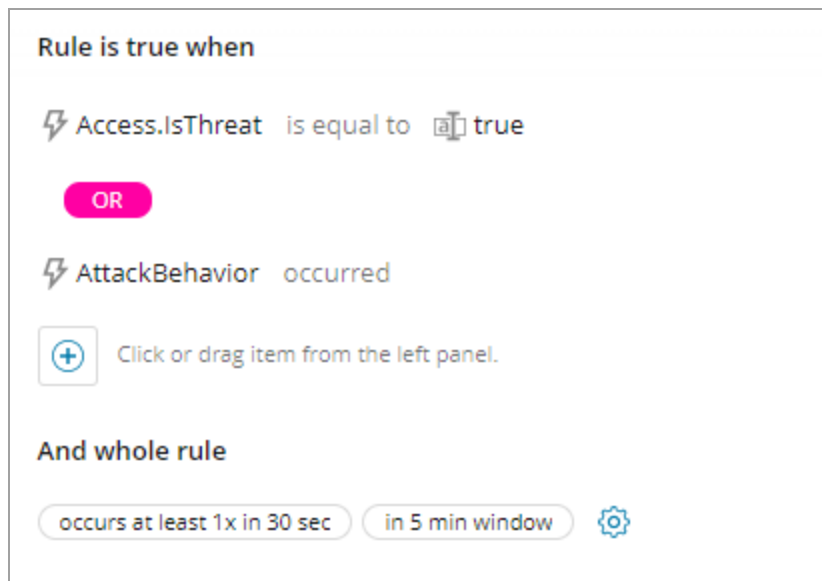
7. After you configure part of a rule, you can change it by moving the cursor over it to display the rule builder toolbar.



This enables you to:

- Apply [occurrence settings](#) for this part of the rule by clicking the  icon
 - [Edit the expression](#) by clicking the  icon
 - Delete the expression by clicking the  icon
 - Add an addition entity or entity field by clicking the  icon
8. To add subsequent rule parts, click the rule definition , and then create the condition as shown above.
 9. From the drop-down list, select an option, enter a specific value or keyword directly.

To change an And operator, click And, and then select Or.



By default, the actions are triggered whenever the conditions that make up the rule are true. However, you can change this so that the rule has to be true multiple times. For more information, see [Occurrence settings](#).

10. Click Next to display Details and actions.

Create new rule

Rule definition

Details and actions

Details and actions

Rule name

Austin23 server accessed out of office hours

Rule description (optional)

Tags

Inappropriate Usage

+ Add tag

OPTIONS

Enable rule after saving

Enable test mode

Use rule without triggering actions

ACTIONS

+ Add new action

At least one action have to be defined

Cancel

Back

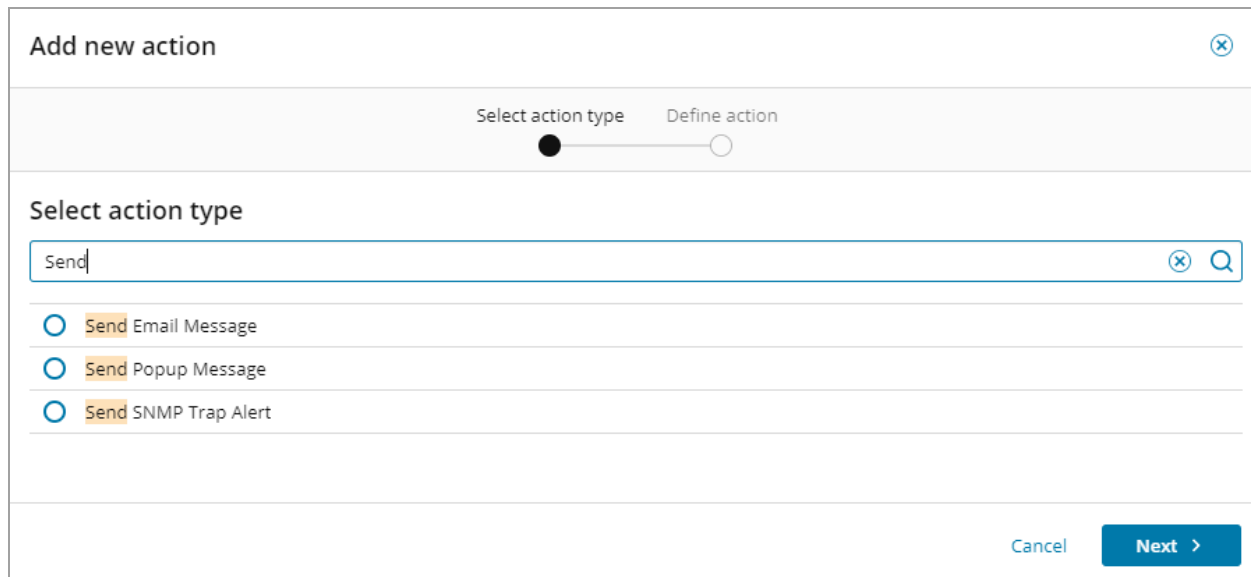
Create

11. Under Details and actions, enter a rule name and optional description.

12. Click the  icon to select one or more optional tags for this rule.

 Tags make it easier to catalog and find rules.

13. Turn off the Click Enable rule after saving THIS option if you want to save a rule without adding an action. You can enable the rule afterwards from the Rules screen.
14. Turn on the Enable test mode option if you want to use this rule test mode. The rule will run but will not trigger any actions. This option allows you to view how the activated rule will behave without disrupting your network. You can Identify test mode rules in your list by the Test icon .
15. Click Add new action to add an action when the rule triggers.



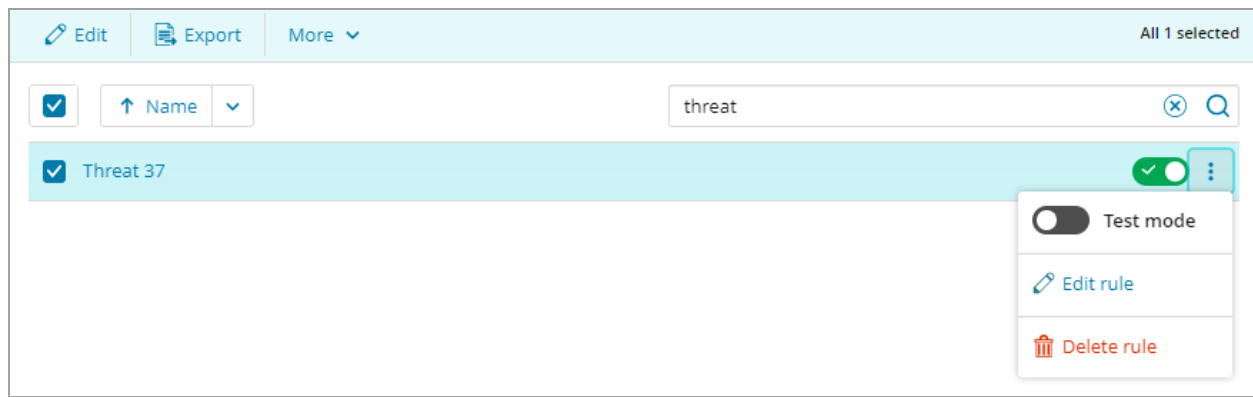
16. Enter a search term or select an action from the list, and then click Next.
17. Define the trigger action, and then click Add.

 SEM provides over 30 actions that can be triggered using rules, ranging from Sending a pop-up message to Disabling Networking. For each the procedure is similar: select or enter the required parameters, and click Add.

You can add multiple actions to a rule by clicking Add new action.

18. Click Create when you have finished adding actions to this rule. The rule is now available in the list of rules.

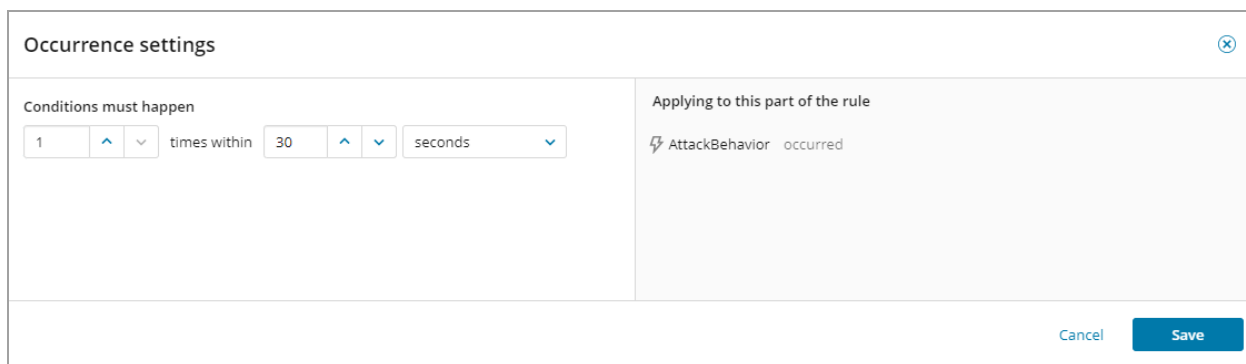
To edit, delete, and toggle test mode, click the vertical ellipsis next to a rule.



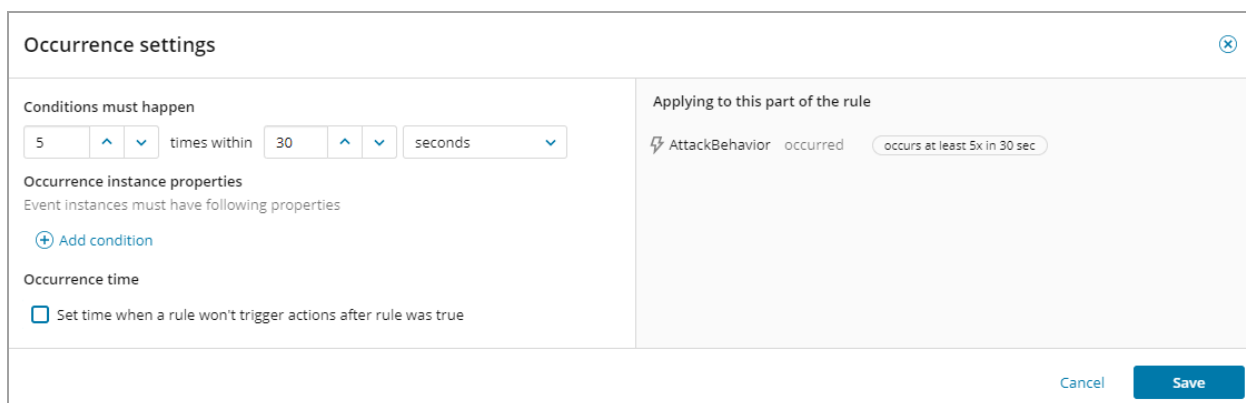
Configure the occurrence settings

By default, a condition must occur once to satisfy part of a rule. You can change this using the occurrence setting. For example, you can know if an occurrence happens five times in thirty seconds.

To apply occurrence settings for this part of the rule, click the  icon on the SEM rule builder tool bar.



If you change the number of times this condition occurs to satisfy this part of the rule, the window is expanded as shown below.



You can also specify additional conditions. For example the following would be true if the event occurred twice within ten minutes with the same DetectionIP.

Occurrence settings

Conditions must happen

2

↑

↓

times within

10

↑

↓

minutes

Occurrence instance properties

Event instances must have following properties

AttackBehavior

with same

DetectionIP

[+ Add condition](#)

Occurrence time

☐ Set time when a rule won't trigger actions after rule was true

Applying to this part of the rule

⚡ AttackBehavior occurred

[Cancel](#)
[Save](#)

You can additionally set a period that must elapse before this part of the rule can be triggered again by checking the Occurrence time box.

Edit the expressions

To change the expression for a rule part, click the  icon on the SEM rule builder tool bar. A popup window is displayed showing the components of the expression. For an entity, this will show two field: the entity name and whether or not the condition occurred. For an entity field, the following fields are displayed.

Rule is true when

⚡ AttackBehavior.Severity is equal to

5

⚙️

✏️

🗑️

+

+

Click or drag item from the left

And whole rule

occurs at least 1x in 30 sec

in 5

⚡ AttackBehavior

Severity

is equal to

Number

5

↑

↓

Cancel

Save

Create a rule from a rules template

SEM comes with over 30 predefined templates that can be easily adapted to your precise requirements.

- Create rule from template

Select rule template

Review rule condition

Rule details

Select rule template

Filter icon

↑ Name ↓

web traffic

Anonymous Web Traffic

Web Traffic Content Filter

Web Traffic Content Filter Infer HTTP Client Access alert

Network

Proxy Servers and Co...

Firewalls

+6

Network

Firewalls

Routers/Switches

Network

Firewalls

Routers/Switches

Cancel

Next >

- Create rule from template

Select rule template

Review rule condition

Rule details

Review rule condition

WebTrafficAudit.URL is in Anonymizer Web Sites

And whole rule

occurs at least 1x in 30 sec in 5 min window

Cancel

Edit rule

Back

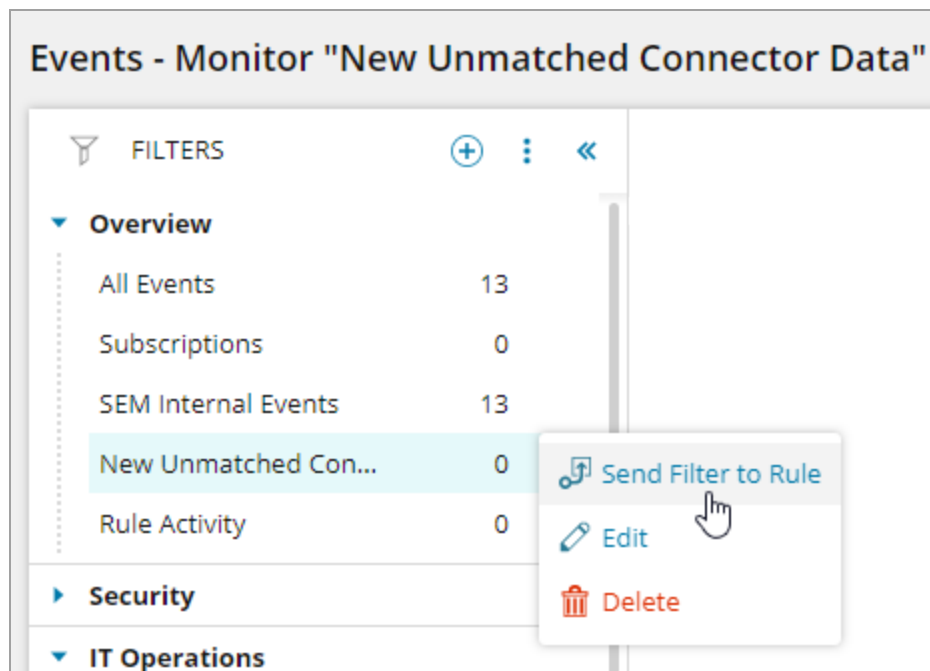
Next

5. Review the existing conditions and values, and click Edit Rule if you need to change these.
See [Create a rule](#) for instructions on how to change the rule settings.
6. After you update the rule, click Next.
7. Review and adjust the rule details and actions where needed, and then click Create.

Create a rule from a filter

From the Filters pane, you can create a new rule based on any existing filter with a single click. This allows you to set alerts for specific event activity without manually duplicating filter values in the custom rule builder.

1. Log in to the SEM Console.
2. On the toolbar, click Live Events.
3. In the Filters pane, scroll down to locate your filter.
4. Hover over the filter to expose the vertical ellipsis.
5. Click the ellipsis and select Send Filter to Rule.



The rule builder displays the existing filter values.

Rule definition

Details and actions

Rule is true when

⚡ Incident occurred

OR

⚡ HostIncident occurred

OR

⚡ HybridIncident occurred

OR

⚡ NetworkIncident occurred

+

Click or drag item from the left panel.

And whole rule

occurs at least 1x in 30sec

in 5min window

⚙

☐ Set time when a rule won't trigger actions after rule was true

6. To complete the rule configuration.

See [Create a new rule](#) for instructions.

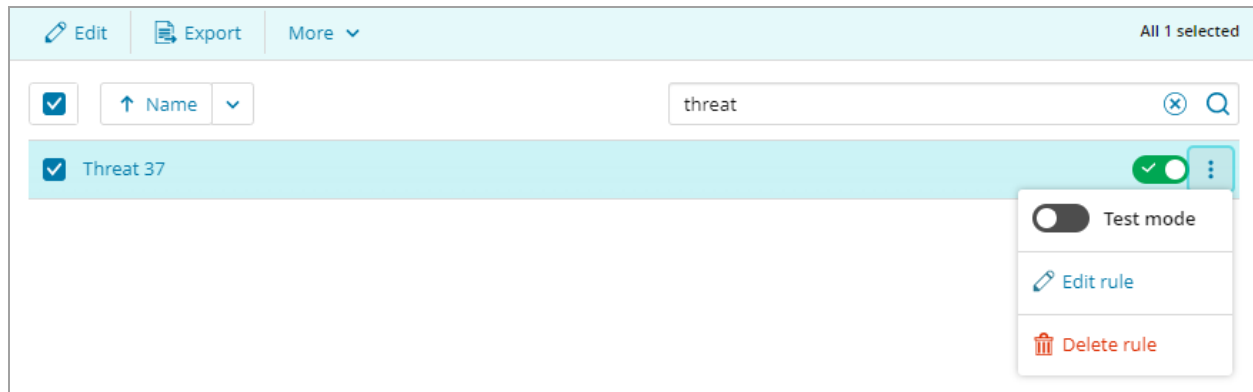
! If you apply rule definition changes to a rule created from a filter, the changes are not reflected in the existing filter. If the filter changes, the associated rule is not updated with the filter changes.

Test, enable, and disable rules in SEM

i See [Create a new rule](#) for instruction on how to create a rule.

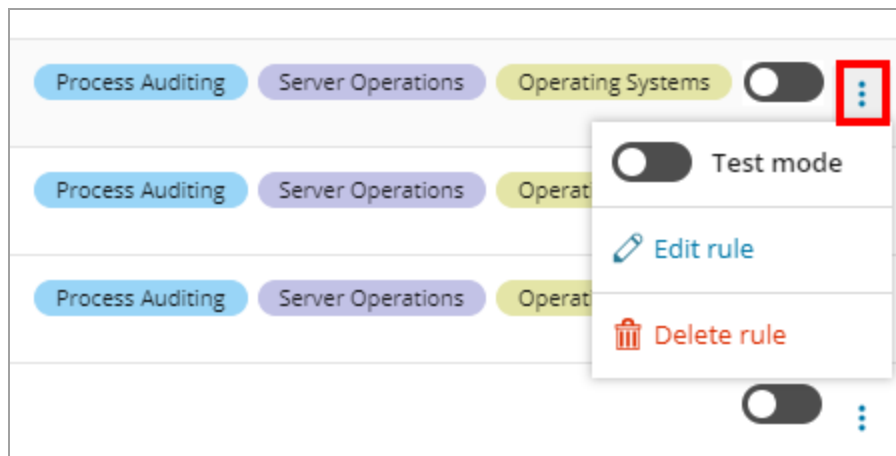
1. Log in to the SEM Console.
2. On the toolbar, click the Rules tab.

3. To disable a rule, click the enabled toggle button next to a rule. To edit, delete, and toggle test mode, click the vertical ellipsis next to a rule.



Enable rules from the rules builder

1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. Click the vertical ellipsis next to a rule, and then select Edit rule.



4. Click Next.

5. Under details and actions, click the toggle button to enable the rule after saving, and then click Save.

Create new rule

Rule definition

Details and actions

Details and actions

Rule name

Austin23 server accessed out of office hours

Rule description (optional)

Tags

Inappropriate Usage

Add tag

OPTIONS

Enable rule after saving

Enable test mode

Use rule without triggering actions

ACTIONS

Add new action

At least one action have to be defined

Cancel

Back

Create

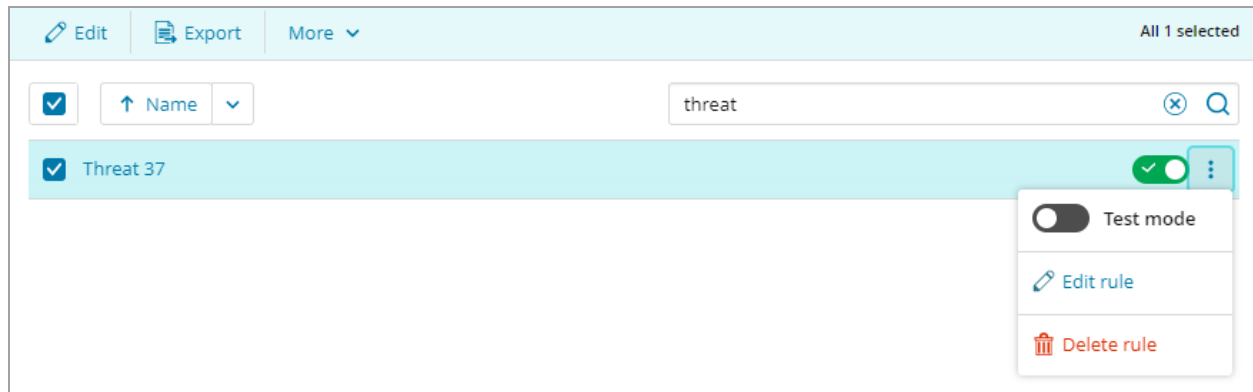
Test rules in SEM

Before you put a rule into production, try it out in test mode. In this mode, the SEM Manager processes the rule alert messages, but does not execute any rule actions. This process allows you to see how the activated rule will behave without disrupting your network.

Enable or disable test mode in the Rules list

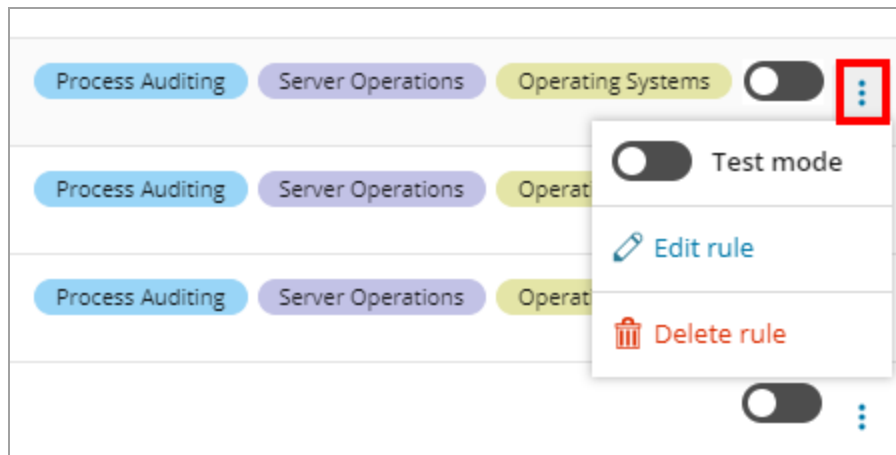
1. Log in to the SEM Console.
2. On the toolbar, select Rules.
3. To disable a rule, click the enabled toggle button next to a rule.

To enable or disable test mode, click the vertical ellipsis next to a rule, and then toggle Test mode.



Enable or disable test mode from the rules builder

1. Log in to the SEM Console.
2. On the toolbar, click the Rules tab.
3. Click the vertical ellipsis next to a rule, and then select Edit rule.



4. Click Next.

5. Under Details and actions, click the toggle switch to enable or disable test mode, and then click Save.

Create new rule

Rule definition

Details and actions

Details and actions

Rule name

Austin23 server accessed out of office hours

Rule description (optional)

Tags

Inappropriate Usage

+ Add tag

OPTIONS

✓ Enable rule after saving

Enable test mode

Use rule without triggering actions

ACTIONS

+ Add new action

At least one action have to be defined

Cancel

Back

Create

Disable rule processing in SEM

The SEM Manager continues to use active rules if they are enabled. Turn off rules by disabling the rules.

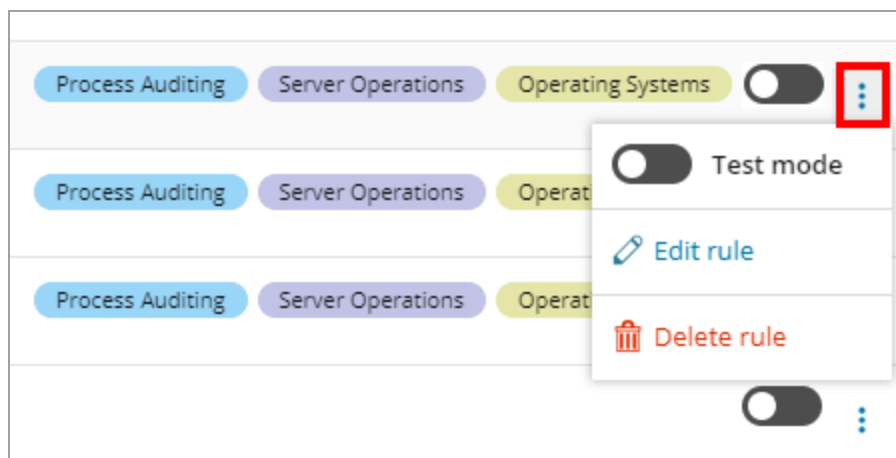
Disable rules from the Rules list

1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. To disable a rule, click the enabled toggle button next to the rule.

See [Create a new rule](#) for more information.

Disable rules from the Rules builder

1. On the SEM Console, select Rules.
2. Click the vertical ellipsis next to a rule, and then select Edit rule.



3. Click Next.

- Under details and actions, toggle off the Enable the rule after saving, and then click Save.

Create new rule

Rule definition

Details and actions

Details and actions

Rule name

Austin23 server accessed out of office hours

Rule description (optional)

Tags

Inappropriate Usage

+ Add tag

OPTIONS

Enable rule after saving

Enable test mode

Use rule without triggering actions

ACTIONS

+ Add new action

At least one action have to be defined

Cancel

Back

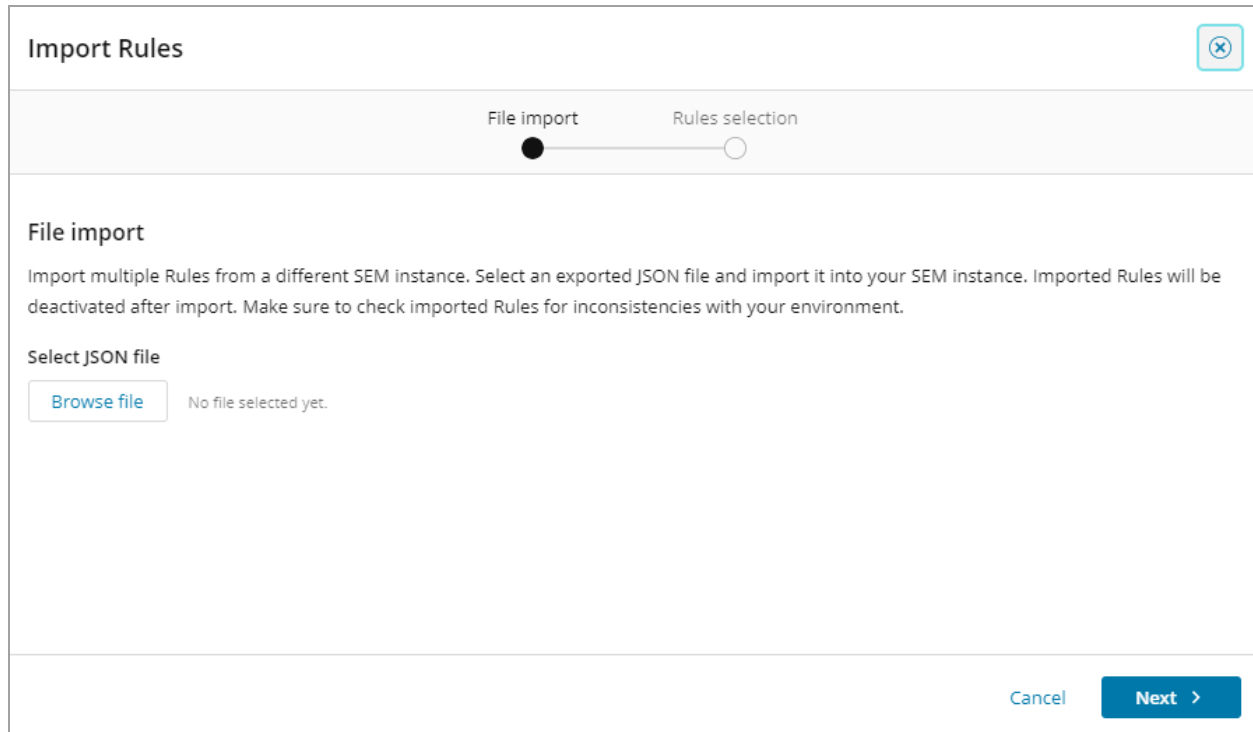
Create

Import and export SEM rules

This section describes how to [import](#) and [export](#) SEM rules in JSON format.

Import SEM rules

1. Log in to the SEM Console.
2. On the toolbar, click the Rules tab.
3. On the Rules toolbar, click Import to display the Import Rules window.



Import Rules

File import Rules selection

File import

Import multiple Rules from a different SEM instance. Select an exported JSON file and import it into your SEM instance. Imported Rules will be deactivated after import. Make sure to check imported Rules for inconsistencies with your environment.

Select JSON file

[Browse file](#) No file selected yet.

[Cancel](#) [Next >](#)

4. Click Browse file and navigate to the JSON file containing the SEM rules.
5. Click Next.

The list of rules in the selected file is displayed.

Depending on the number of rules there may be a brief delay before the next screen is displayed.

Import Rules

File import Rules selection

Rules selection

Search...

☒ Agent Offline Timeouts
Agent offline but not online within 2 minutes

☐ All Network Traffic
This rule is copied from the Fileless Rule functionality...

Server Operatio... General Best Pr... Operating System...

No action defined

Cancel < Back Import

You can sort, filter, and search this list. Initially, all rules are selected for import, but you can select or unselect all or specific rules as required.

 You cannot import invalid rules. If any rules are invalid, a message displays describing how many rules are invalid. These rules display in gray with message explaining why they are invalid.

- After you select the rules you want to import, click Import.

If your selected rules include identical names, the following window displays, prompting you to skip, overwrite, or rename the imported rule.

Import Rules

File import

Rules selection

Conflicts

Conflicts

Following Rules already exist in SEM instance. Select how SEM should handle these conflicts.

Agent Offline Timeouts

☒ Skip
 ☐ Overwrite
 ☐ Rename

Cancel

Back

Import

- When you are finished, click Import.

The Imported Results window displays with a list of your imported rules.

Import Results

Imported successfully


 Agent Offline Timeouts
 Agent offline but not online within 2 minutes

Server Operatio...

General Best Pr...

Operating Syste...

Item was overwritten

Close

- Click Close to return to the complete list of rules.

Export SEM rules

- In the Rules window toolbar, click Export All.
- In the Save As window, navigate to the required directory, enter a name for the exported rules file, and click Save.

Create email templates for use with SEM rules

Email templates are pre-formatted messages sent to users when alert events trigger a rule. You can use email templates to customize your email notifications triggered as responses in your rules.

An email template includes static and dynamic text (or parameters). The static text allows you to customize the email design. The dynamic text is created from the original event that triggered the rule to fire.

Report specific information

Create email templates to report specific information about an alert event and variables that capture specific parameters about that event. For example, you can report which server is affected, what time the event occurred, or which agent was shut down. Additionally, you can create an Account Lockout template to notify key personnel when an account is locked out or automatically file a trouble ticket. Create static text to describe the event, and incorporate dynamic text that provides the account information from the original event.

Address specific event types

Create templates that are specific to an event type to avoid having to create one email template per rule. For example, you can have one template for Account Modification that can provide a notification when a user is added or removed from a group, when a password is reset, or when other account details are changed. There is no limit to the number of templates you can create.

Best practices

To keep rules, events, and emails simple to manage, SolarWinds recommends the following:

- Create the rule with a name that describes the event.
- Create the email template with a name that describes the event.
- In the email template subject or message, enter the event or rule name to describe the event or alert.

When you receive the email, you can identify the email template, the rule that fired, and the event that caused the rule to fire.

Create or edit an email template

You can use email templates to customize your email notifications when triggered as responses in your custom rules. An email template includes static and dynamic text (or parameters). The static text lets you customize the message body of the email. The dynamic text is filled in from the original event that caused the rule to fire.

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Email Templates
3. On the Email templates toolbar, click Create Email template.
4. Complete the fields in the Create Email template window.

Create Email template

Email template name

Email template name is required.

Subject

Message

Add parameter

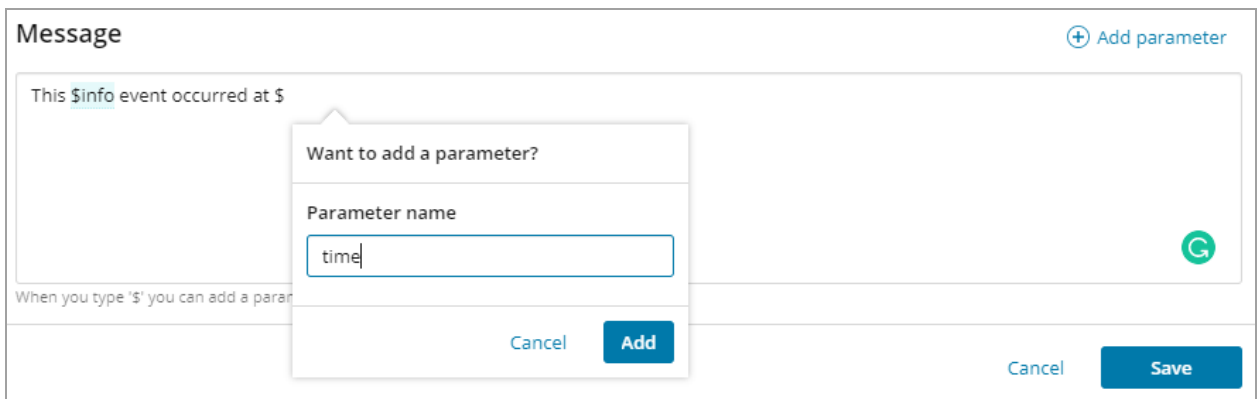
When you type '\$' you can add a parameter to the template.

Cancel

Create

- a. In the Email template name field, enter a descriptive name for the template.
- b. In the Subject field, enter the subject of the template email.
- c. In the Message field, enter the text of the message to be included in this email. This text is static and cannot be edited within emails created from this template. However, you can include parameters which are replaced by the appropriate metrics (or string) when an email is generated by a rule that uses this template.

To add parameters, either type \$ or click Add parameter, then add the parameter. You do not need to specify the values here, and can use any combination of letters, number and the ".", "_", and "-" characters.



Message

+ Add parameter

This \$info event occurred at \$

Want to add a parameter?

Parameter name

time

When you type '\$' you can add a parameter

Cancel Add

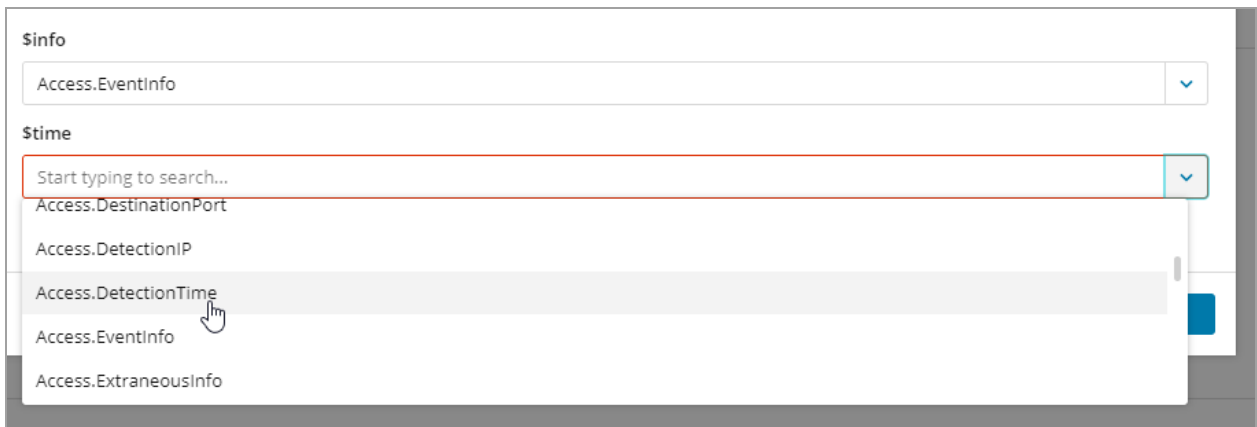
Cancel Save

When you create the rule, the fields that can be substituted for these parameters are displayed. For example, if your message is:

This \$info event occurred at \$time.

You create a rule triggered by Access.IsThreat, which you can assign any of the Access fields to replace the parameters.

i In the Refine Results pane, you can also filter the groups by the modifier and the time last modified.



\$info

Access.EventInfo

\$time

Start typing to search...

Access.DestinationPort

Access.DetectionIP

Access.DetectionTime

Access.EventInfo

Access.ExtraneousInfo

5. Click Create to save your template.

The new template is now available as an action type in your custom rule builder. See [Create a new rule](#) for more information.

Example SEM rules

This section provides examples of how to create rules in SEM that monitors and responds to security events in your organization.

See the following topics for examples of SEM rules you can create in your organization.

Create and enable a SEM rule to identify port scanning traffic

To identify suspicious firewall traffic indicative of port scanning, clone and enable the PortScans rule. This rule generates a default TCPPortScan event, which the SEM console displays in the default Security Events filter. Use this event to monitor suspicious network traffic and prevent unauthorized access to your firewall.

1. Log in to the SEM Console.
2. In the toolbar, click Rules.
3. On the Rules toolbar, click Create rule from template.
4. In the search box, enter PortScans.

Create rule from template

Select rule template Review rule condition Rule details

Select rule template

portscans

PortScans

Network Scan Firewalls +9

5. Select the PortScans rule template, and then click Next.
6. Review the existing conditions and values. Click Edit and updated if required.

Create rule from template

Select rule template

Review rule condition

Rule details

Review rule condition

⚡

TCPTrafficAudit

occurred

And whole rule

occurs at least 10x in 30 sec

in 5 min window

same SourceMachine (TCPTrafficAudit)

distinct DestinationPort (TCPTrafficAudit)

7. Click Next.
8. Review and adjust the rule details where needed.

Rule is true when

⚡

TCPTrafficAudit

occurred

+

Click or drag item from the left panel.

And whole rule

occurs at least 10x in 30 sec

in 5 min window

same SourceMachine (TCPTrafficAudit)

distinct DestinationPort (TCPTrafficAudit)

9. Click Create.

 See [Create a new rule](#) for more information.

Create and enable the Known Spyware Site traffic rule

You can track when users attempt to access suspicious websites using partial or complete URL addresses by enabling the Known Spyware Site Traffic rule. This rule generates a HostIncident event by default that you can use in conjunction with the Incidents report to notify auditors that you are auditing critical events on your network.

Before you enable this rule, ensure your proxy server transmits complete URL addresses to your SEM Manager by checking the URL field of any WebTrafficAudit event generated by your proxy server. If your proxy server does not log web traffic events with this level of detail, check the events coming from your firewalls, as they can sometimes be used for this rule as well.

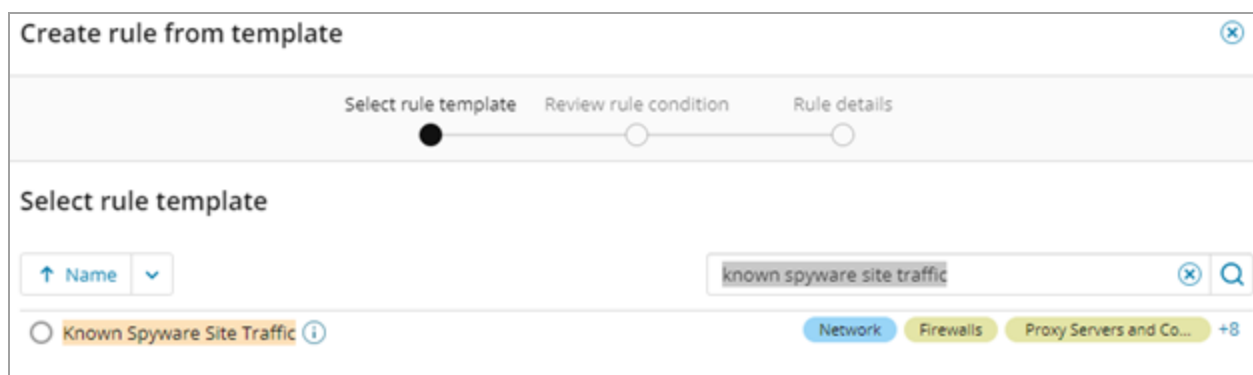
1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. On the Rules toolbar, click Create rule from template.



4. In the search box, enter:

Known Spyware Site traffic

As you type the list of templates is filtered to display your search text.



5. Select the Known Spyware Site Traffic rule template, and click Next.
6. Review and edit the existing conditions and values where needed, and click Next.
7. Review and adjust the rule details where needed, and click Create.

 See [Create a new rule](#) for additional guidance.

Create a SEM rule to track when viruses are not cleaned

Create and enable the Virus Attack – Bad State rule to track virus attacks reported by your anti-virus software. The Bad Virus State User-Defined Group defines a bad state as any virus that is not fully cleaned by your anti-virus software. This includes any virus that is not addressed, quarantined, or renamed.

The default action for this rule generates a HostIncident event, which you can use in conjunction with the Incidents report to notify auditors you are auditing the critical events on your network.

1. Log in to the SEM Console.
2. On the toolbar, click Rules.

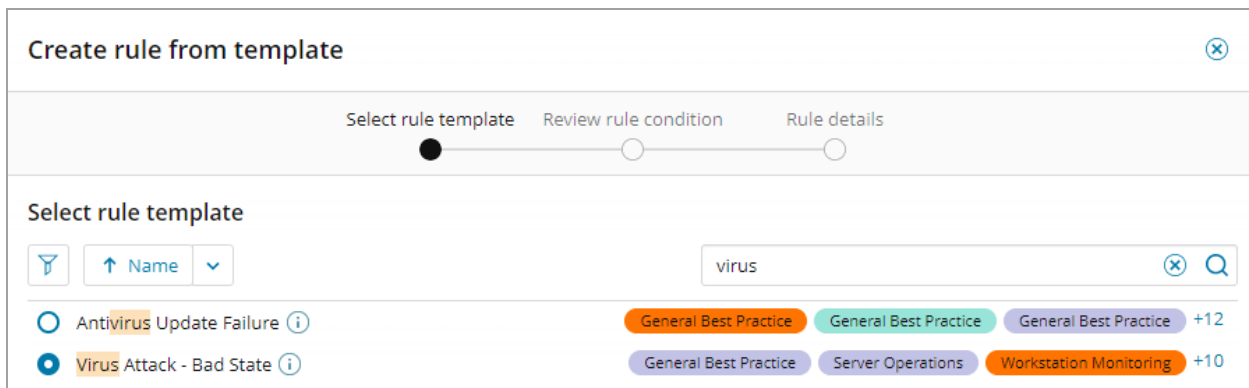
- On the Rules toolbar, click Create rule from template.



- In the search box, enter virus and then click the magnifying glass icon.



- Select the Virus Attack - Bad State rule template, and then click Next.



- Review and edit the existing conditions and values where needed, and then click Next.
- Review and adjust the rule details where needed, and then click Create.

 See [Create a new rule](#) for additional guidance.

Create and enable a critical logon failures rule

Clone and enable critical account logon failures rule to track failed logon attempts to the default Windows Administrator account. The default action for this rule is to generate a HostIncident event, which you can use in conjunction with the Incidents report to notify auditors you are auditing the critical events on your network.

- Log in to the SEM Console.
- On the toolbar, click Rules.
- On the Rules toolbar, click Create rule from template.

Create rule from template

Select rule template

Review rule condition

Rule details

↑ Name

▼

Search...

Agent Offline - Early Shift

Process Auditing

Server Operations

Operating Systems

Agent Offline - Graveyard Shift

Process Auditing

Server Operations

Operating Systems

Agent Offline - Late Shift

Process Auditing

Server Operations

Operating Systems

Agent Offline - Normal Shift

Process Auditing

Server Operations

Operating Systems

Agent Offline - Server

Server Operations

Operating Systems

PCI

+7

Agent Offline Timeout

Server Operations

Operating Systems

General Best Practice

Cancel

Next >

- In the search box, enter:
"critical account" failures
- Select the Critical Account Logon Failures rule template, and then click Next.
- Review and edit the existing conditions and values where needed, and then click Next.
- Review and adjust the rule details where needed, and then click Create.

 See [Create a new rule](#) for additional guidance.

Create and enable a change management rule

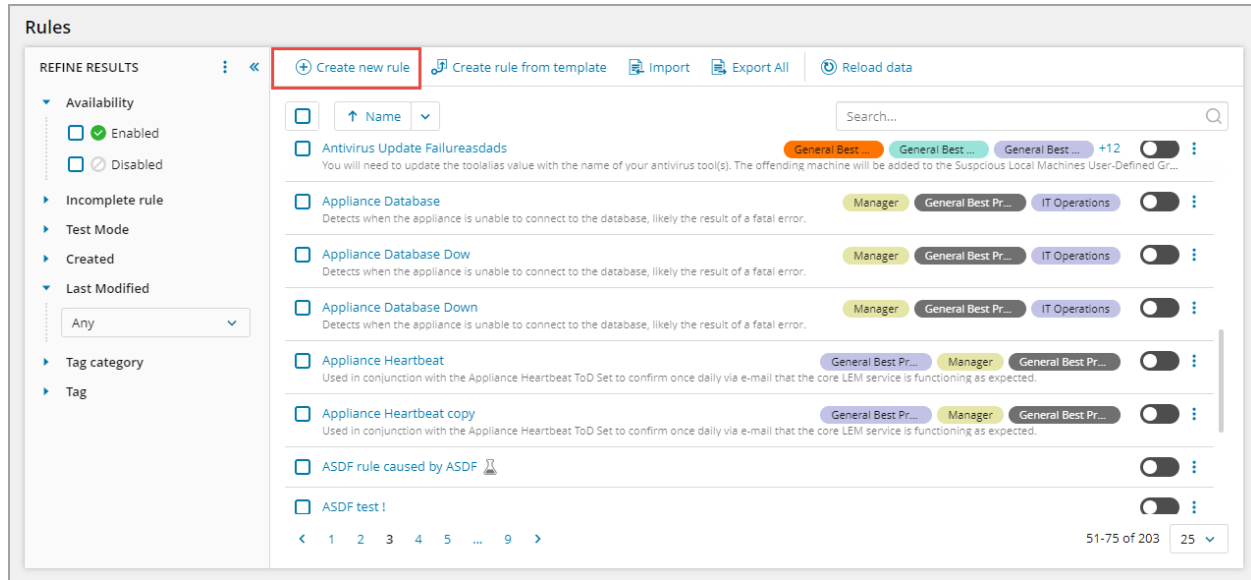
Change management rules notify you when a user makes network configuration changes. For example:

- Adding, changing, or deleting users in Active Directory
- Installing software on monitored computers
- Making changes to the firewall policy

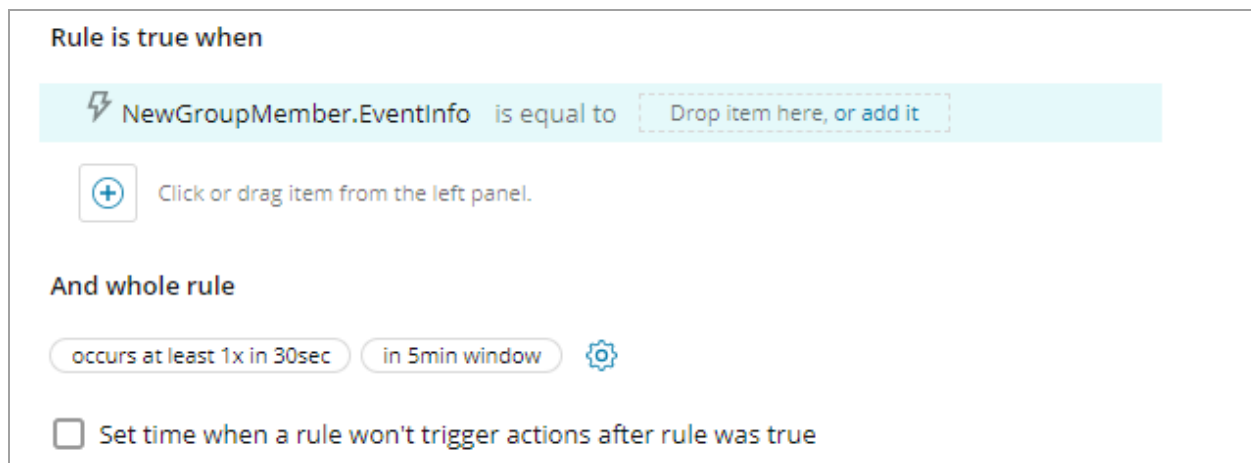
You can create a general change management rule to instruct SEM to notify you when a user changes your network configuration, or you can create a more specific rule that applies to specific users, groups, or types of changes. Generally, if you can see an event in your console, you can create a rule for the event. Use your filters as a starting point for creating custom rules.

- Log in to the SEM Console.
- On the toolbar, click Rules.

- On the Rules toolbar, click Create new rule.



- Under Rule Values, expand the Events group, and then select NewGroupMember.
- Under NewGroupMember fields, locate EventInfo, and then drag it into the rule builder.



- To account for all variations on the word administrator, click the **or add it** hyperlink and enter *admin*.
- Keep the default occurrence and trigger actions settings.
- Click Next.
- Enter an appropriate rule name. For example, New Admin User.
- Under Options, click the toggle button to enable the rule after saving.
- Click Add new action, select Send Email Action, and then click Next.

12. From the Email Template drop-down list, select a template.
13. From the Recipients drop-down list, select one or more recipients, and then click Add.
14. Review your details and actions, and then click Create.

Select an event response from an existing rule

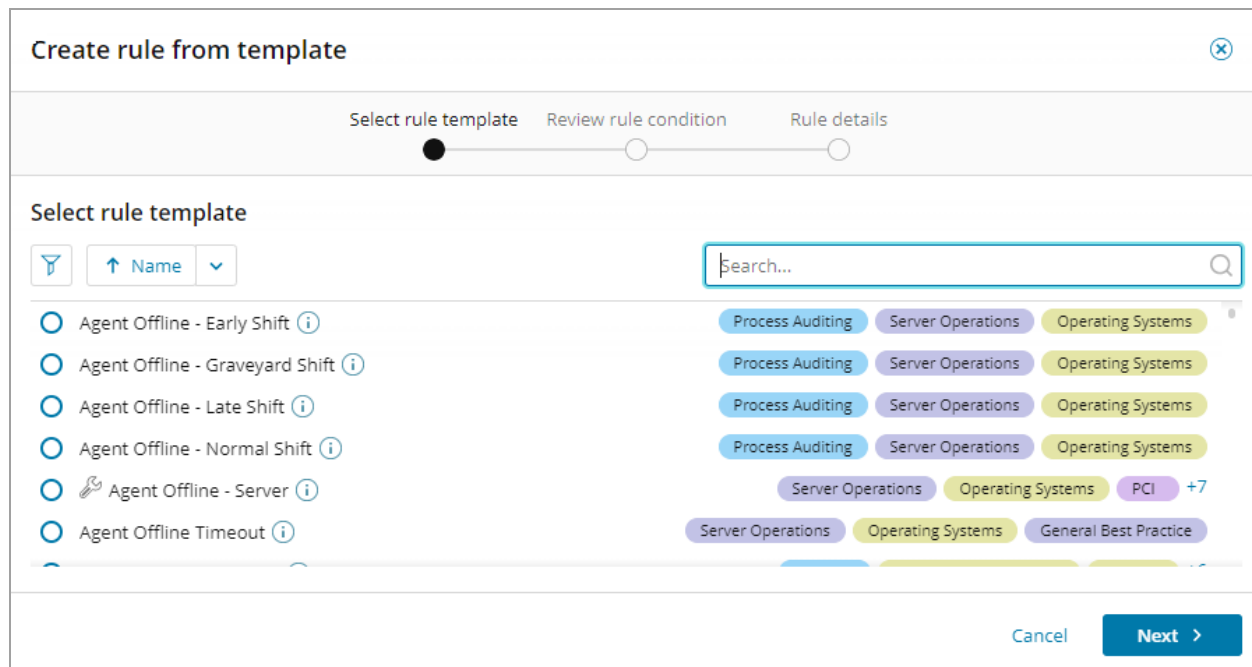
1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. Select a rule in the list, click Edit, and then click Next.
4. Under Actions, click Add new action.
5. Select your response action type, and then click Next.
6. From the Define action drop-down lists, select your options based on the action type, and then click Add.
7. Adjust the details and actions, if needed, and then click Save.

 See [Create a new rule](#) for additional guidance.

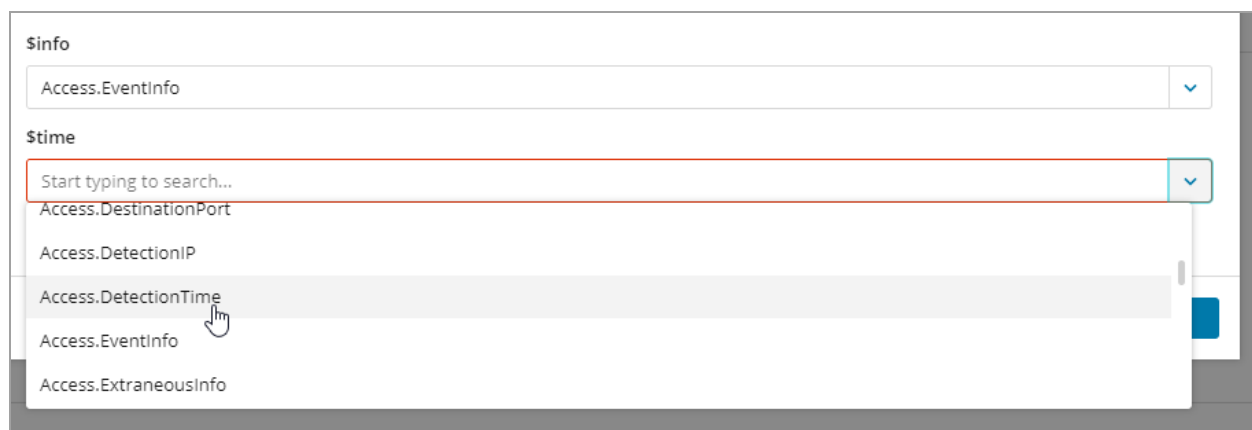
 Learn about response actions [here](#).

Add the Send Email Message action to a rule created from a template

1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. On the Rules toolbar, click Create rule from template.



4. In the search box, enter user account lockout.
5. Select the required rule template, and click Next.
6. Review and edit the existing conditions and values where needed, and then click Next.
7. Under Rule details, click Add new action, select Send Email Message, and select Next..
8. Select an email template and add recipients.
9. Select the data fields to use for any parameters in the email template.

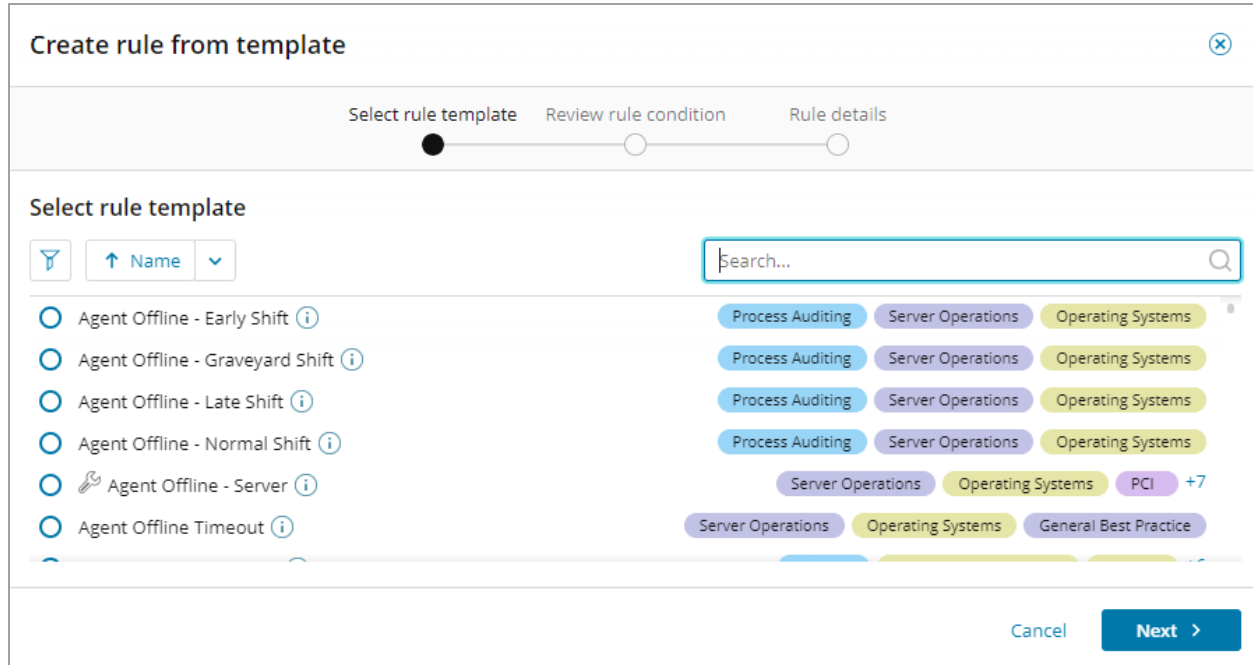


10. Click Add, and then Create.

 See [Create a new rule](#) for additional guidance.

Use the Send Email Message action in SEM rule creation

1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. On the Rules toolbar, click Create rule from template.



Create rule from template ✕

Select rule template Review rule condition Rule details

Select rule template

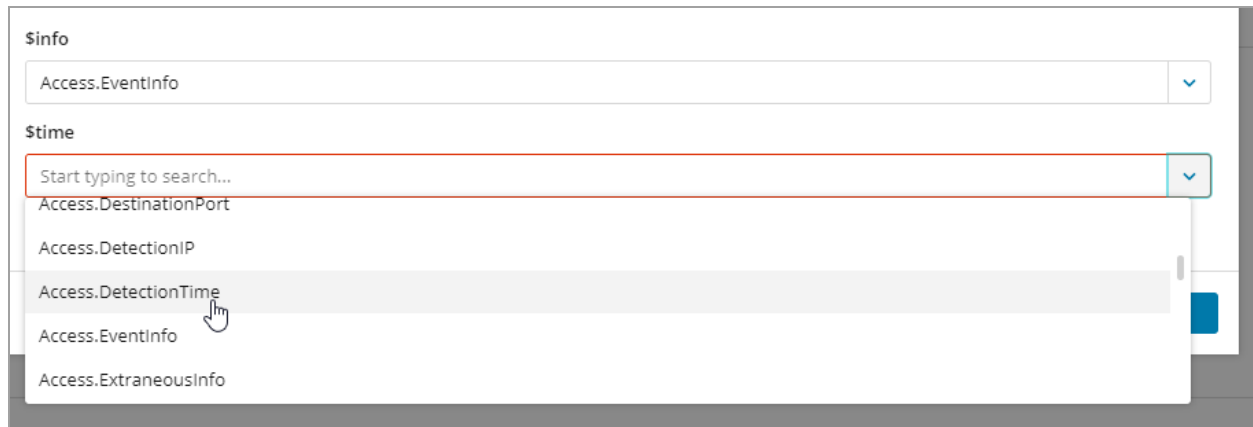
🔍 ↑ Name ▼

- ☐ Agent Offline - Early Shift ℹ
 - Process Auditing
 - Server Operations
 - Operating Systems
- ☐ Agent Offline - Graveyard Shift ℹ
 - Process Auditing
 - Server Operations
 - Operating Systems
- ☐ Agent Offline - Late Shift ℹ
 - Process Auditing
 - Server Operations
 - Operating Systems
- ☐ Agent Offline - Normal Shift ℹ
 - Process Auditing
 - Server Operations
 - Operating Systems
- ☐ Agent Offline - Server ℹ
 - Server Operations
 - Operating Systems
 - PCI
 - +7
- ☐ Agent Offline Timeout ℹ
 - Server Operations
 - Operating Systems
 - General Best Practice

Cancel Next >

4. In the search box, enter user account logout.
5. Select the required rule template, and click Next.
6. Review and edit the existing conditions and values where needed, and then click Next.
7. Under Rule details, click Add new action, select Send Email Message, and select Next..
8. Select an email template and add recipients.

9. Select the data fields to use for any parameters in the email template.



The screenshot shows a web interface with two dropdown menus. The first menu, labeled '\$info', has 'Access.EventInfo' selected. The second menu, labeled '\$time', is open, showing a search bar with the text 'Start typing to search...' and a list of options: 'Access.DestinationPort', 'Access.DetectionIP', 'Access.DetectionTime' (which is highlighted and has a mouse cursor over it), 'Access.EventInfo', and 'Access.ExtraneousInfo'.

10. Click Add, and then Create.

 See [Create a new rule](#) for additional guidance.

Create response actions for network and system events

This section describes how to create response actions in the SEM Console for network and system events.

About SEM response actions

 See [Create a new rule](#) to learn how to create an active response rule.

About SEM active response

An active response (also called an event response) is a SEM action in response to suspicious activity or an attack. Active response actions include the Block IP active response, the Disable Networking active response, the Log off User active response, the Kill Process active response, the Detach USB Device active response, and so on.

The Select action type list in the rules builder provides a list of actions you can execute for a specific event. Each Respond command opens the Respond form. This form includes data from the field you selected and options for customizing the action—similar to configuring the active response for a rule in the Rule Creation.

The Respond menu is context-sensitive. The event type or cell currently selected in the event grid determines which responses you can choose.

Select an event response from an existing rule

1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. Select a rule in the list, click Edit, and then click Next.
4. Under Actions, click Add new action.
5. Select your response action type, and then click Next.
6. From the Define action drop-down lists, select your options based on the action type, and then click Add.
7. Adjust the details and actions, if needed, and then click Save.

 See [Create a new rule](#) for additional guidance.

Use SEM active responses to perform Windows actions related to users, groups, and domains

Use the following user-based active responses to perform Windows-based actions related to users, groups, and domains on your SEM Agents.

- Add Domain User To Group
- Add Local User To Group
- Create User Account
- Create User Group
- Delete User Account
- Delete User Group
- Disable Domain User Account
- Disable Local User Account
- Enable Domain User Account
- Enable Local User Account
- Log Off User
- Remove Domain User From Group
- Remove Local User From Group
- Reset User Account Password

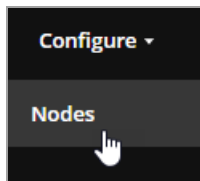
These actions are useful to respond to unauthorized change management activity and to automate user-related maintenance. They can be automated in a SEM rule, or executed manually from the Respond menu on the SEM Console.

Configure an active response connector on a SEM agent

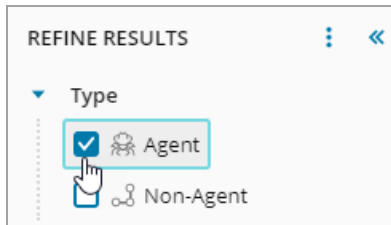
Configure the Windows active response connector on each SEM agent that requires active responses.

You can deploy your SEM agents and configure the Windows active response connector based on where you want to perform these actions. To perform actions at the domain level, deploy a SEM agent to at least one domain controller. To perform actions at the local level, deploy a SEM agent to each computer that requires a response.

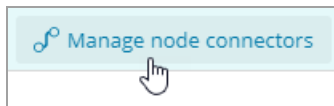
1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.



3. In the Refine Results column, expand Type and select the Agent check box.



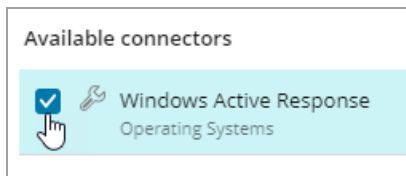
4. Select an agent, and then click Manage node connectors.



5. In the search box, type Windows Active Response and then click the magnifying glass icon.



6. Under Available connectors, select the Windows Active Response connector.



7. Click Add Connector.



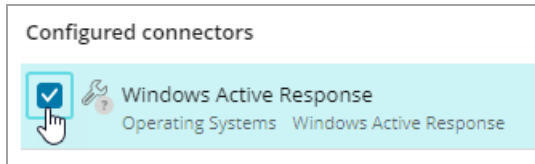
8. Enter a custom alias name for the new connector, or accept the default.

Name
Windows Active Response
Connector name

9. Click Add.



10. Under Configured connectors, select your configured connector.



11. Click Start.



The green indicator next to the connector name displays, indicating that the connector is started and running.

Actions SEM can take to respond to events

The following table lists the various actions a SEM Manager can take to respond to events. These actions are configured in the Respond form when you are initiating an active response, and in the rules window's Actions box when you are configuring a rule's automatic response.

The table's Action column lists the actions that are available. They are alphabetized for easy reference. The Description column briefly states how the action behaves. The Fields column lists the primary data fields that apply with each action. Some data fields will vary, depending on the options you select.

Action	Description	Fields
Add Domain User To Group	This action adds a domain user to a specified user group that resides on a particular Agent.	Domain Controller Agent Select the event field or constant that defines the Agent on which the group to be modified resides. To modify a group at the domain level, specify a domain controller as the Agent. Group Name Select the event field or constant that defines the group that is to be modified. Username Select the event field or constant that defines the user who is to be added to the group.
Add Local User To Group	This action adds a local user to a specified user group that resides on a particular Agent.	Agent Select the event field or constant that defines the Agent on which the group to be modified resides. To modify a group at the domain level, specify a domain controller as the Agent. Group Name Select the event field or constant that defines the group that is to be modified. Username Select the event field or constant that defines the user who is to be added to the group.
Add User-Defined Group Element	This action adds a new data element to a particular user-defined group.	User-Defined Group Element From the User-Defined Groups list, select the User-Defined Group that is to receive the new data Element. Value Select the event field or constant that defines the data element that is to be added to the specified User-Defined Group. The fields will vary according to which User-Defined Group you select.

Action	Description	Fields
Append Text To File	This action appends text to a file. This allows you to data from an event and put it in a text file.	Agent Select the event field or constant that defines the Agent on which the file to be appended is located. File Path Select the event field or constant that defines the path to the Agent file that is to be appended with text. Text Select the event field or constant that defines the text to be appended to file.
Block IP	This action blocks an IP address.	IP Address Select the event field or constant that identifies the device's IP address.
Create User Account	This action creates a new user account on an Agent.	Agent Select the event field or constant that defines the Agent on which the new user account is to be added. To create a user account at the domain level, specify a domain controller as the Agent. Account Name Select the event field or constant that names the account that is to be created. Account Password Select the event field or constant that defines the password that is to be assigned to the new account.

Action	Description	Fields
Create User Group	This action creates a specified user group on an Agent. A user group is a new group of Windows users on a Windows PC, server, or network who are external to the SEM system.	Agent Select the event field or constant that defines the Agent on which the new user group is to reside. To create a user group at the domain level, specify a domain controller as the Agent. Group Name Select the event field or constant that defines which user group is to be created.
Delete User Account	This action deletes a user account from an Agent.	Agent Select the event field or constant that defines the Agent on which the user account is to be deleted. To delete a user account at the domain level, specify a domain controller as the Agent. Account Name Select the event field or constant that names the account that is to be deleted.
Delete User Group	This action deletes a user group from a particular Agent.	Agent Select the event field or constant that defines the Agent on which the user group to be deleted resides. To delete a user group at the domain level, specify a domain controller as the Agent. Group Name Select the event field or constant that defines the user group that is to be deleted.
Detach USB Device	This action detaches a USB mass storage device that is connected to an Agent.	Agent Select the event field or constant that defines the Agent from which the USB device is to be detached. Device Select the event field or constant that defines the device ID of the USB device that is to be detached.

Action	Description	Fields
Disable Domain User Account	This action disables a Domain User Account on a Domain Controller Agent.	Domain Controller Agent Select the event field or constant that defines the Domain Controller Agent on which the domain user is to be disabled. Destination Account Select the event field or constant that defines the account that is to be disabled.
Disable Local User Account	This action disables a local user account on an Agent.	Agent Select the event field or constant that defines the Agent on which the local user is to be disabled. Destination Account Select the event field or constant that defines the account that is to be disabled.
Disable Networking	This action disables an Agent's network access. The result is that the specified Agent will be unable to connect to the network.	Agent Select the event field or constant that defines the Agent that is to be disabled from the network. Message Type the message that is to appear on the Agent.
Disable Windows Machine Account	This action disables a Windows machine account that resides on a Domain Controller Agent.	Domain Controller Agent Select the event field or constant that defines the Domain Controller Agent on which the account is to be disabled. Destination Account Select the event field or constant that specifies which Windows account is to be disabled.

Action	Description	Fields
Enable Domain User Account	This action enables a Domain User Account on a Domain Controller Agent.	Domain Controller Agent Select the event field or constant that defines the Domain Controller Agent on which the domain user is to be enabled. Destination Account Select the event field or constant that defines the account that is to be enabled.
Enable Local User Account	This action enables a local user account on an Agent.	Agent Select the event field or constant that defines the Agent on which the local user is to be enabled. Destination Account Select the event field or constant that defines the account that is to be enabled.
Enable Windows Machine Account	This action enables a Windows machine account that resides on a Domain Controller Agent.	Domain Controller Agent Select the event field or constant that defines the Domain Controller Agent on which the account is to be enabled. Destination Account Select the event field or constant that specifies which Windows account is to be enabled.
Incident Event	This action escalates potential issues by creating an Incident Event.	Event Select which Incident Event the rule is to create. Event Fields From the list pane, select the events and constants that define the appropriate data elements for each event fields The fields vary, depending on which Incident Event is selected.

Action	Description	Fields
Infer Event	This action escalates potentially irregular audit traffic into security events by creating (or inferring) a new event with a higher severity.	Event Select which Event the rule is to infer. Event Fields From the list pane, select the events and constants that define the appropriate data elements for each event field. The fields vary, depending on the which event is selected.
Kill Process by ID	This action terminates the specified process on an Agent by using its process ID value.	Agent Select the event field or constant that defines the Agent on which the process is to be terminated. Process ID Select the event field or constant that identifies the ID number of the process that is to be terminated.
Kill Process by Name	This action terminates the specified process on an Agent by referring to the process name.	Agent Select the event field or constant that defines the Agent on which the process is to be terminated. Process Name Select the event field or constant that identifies the name of the process that is to be terminated. Account Name Select the event field or constant that identifies the name of the account that is running the process to be terminated.
Log Off User	This action logs the user off of an Agent.	Agent Select the event field or constant that defines the Agent from which the user is to be logged off. Account Name Select the event field or constant that identifies the specific account name that is to be logged off.

Action	Description	Fields
Modify State Variable	This action modifies a state variable.	State Variable From the State Variables list, drag the state variable that the rule is to modify. State Variable Fields From the appropriate component list, type or drag the data element that is to be modified in the state variable. The fields vary, depending on the which state variable is selected.
Remove Domain User From Group	This action removes a domain user from a specified user group that resides on a particular Agent.	Domain Controller Agent Select the event field or constant that defines the domain controller Agent on which the group to be modified resides. Group Name Select the event field or constant that defines the group that is to be modified. User Name Select the event field or constant that defines the user who is to be removed from the group.
Remove Local User From Group	This action removes a local user from a specified user group that resides on a particular Agent.	Agent Select the event field or constant that defines the Agent on which the group to be modified resides. Group Name Select the event field or constant that defines the group that is to be modified. User Name Select the event field or constant that defines the user who is to be removed from the group.

Action	Description	Fields
Remove User-Defined Group Element	This action removes a data element from a particular user-defined group.	User-Defined Group From the User-Defined Groups list, select the user-defined group from which the specified data element is to be removed. Value Select the event field or constant that defines the data element that is to be removed from the specified user-defined group. The fields will vary according to which user-defined group you select.
Reset User Account Password	This action resets a user account password on a particular Agent.	Agent Select the event field or constant that identifies the Agent on which the user password is to be reset. To reset an account at the domain level, specify a domain controller as the Agent. Account Name Select the event field or constant that identifies the user account that is to be reset. New Password Select the event field or constant that defines the user's new password.
Restart Machine	This action reboots an Agent.	Agent Select the event field or constant that identifies the Agent that is to be rebooted. Delay (sec) Type the time (in seconds) after the event occurs that the Manager is to wait before rebooting the Agent.

Action	Description	Fields
Restart Windows Service	This action restarts the specified Windows service on an Agent.	Agent Select the event field or constant that identifies the Agent on which the Windows service will be restarted. Service Name Select the event field or constant that identifies the name of the service that is to be restarted.
Send Email Message	This action sends a preconfigured email message to a predetermined email distribution list.	Email Template Select the template that the email message is to use. Recipients Click the check boxes to select which users are to receive the email message. Email Fields Either drag a field from the components list, or select a constant from the components list to select the appropriate data elements that are to appear in each email template field. The fields vary, depending on which email template is selected.
Send Popup Message	This action displays a pop-up message to an Agent.	Agent Select the event field or constant that identifies the Agent that is to receive the pop-up message. Account Name Select the event field or constant that identifies the user account to receive the message. Message Select the event field or constant that defines the message that is to appear on the Agent's monitor.

Action	Description	Fields
Shutdown Machine	This action shuts down an Agent.	Agent Select the event field or constant that identifies the Agent that is to be shut down. Delay (sec) Type the time (in seconds) after the event occurs that the Manager is to wait before shutting down the Agent.
Start Windows Service	This action starts the specified Windows service on an Agent.	Agent Select the event field or constant that identifies the Agent on which the Windows service is to be started. Service Name Select the event field or constant that defines the Windows service that is to be started.
Stop Windows Service	This action stops the specified Windows service on an Agent.	Agent Select the event field or constant that identifies the Agent on which the Windows service is to be stopped. Service Name Select the event field or constant that defines the Windows service that is to be stopped.

Use computer-based active responses in SEM

To perform Windows-based actions related to computers and computer services on your SEM agents, employ the following Computer-based active responses in your deployment:

- Disable Windows Machine Account1
- Enable Windows Machine Account1
- Disable Networking
- Detach USB Device
- Restart Machine
- Restart Windows Service
- Send Popup Message
- Shutdown Machine

- Start Windows Service
- Stop Windows Service

These actions can help you respond to insider abuse, computer infections, and other suspicious activity. They can be automated in a SEM rule, or executed manually from the Respond menu on the SEM Console.

Requirements

Configure the Windows Active Response connector on each SEM agent that responds to the active responses.

Deploy your SEM agents and configure the Windows Active Response connector based on where you want to perform these actions. To perform actions at the domain level, deploy a SEM agent on at least one domain controller. To perform actions at the local level, deploy a SEM agent on each computer you want to respond to when action is required.

Use the Append Text to File active response in SEM

Use the Append Text To File active response to append static or dynamic text to a flat text file in your network. This action helps you keep a running list of deployed SEM agents or track certain types of activity across several users and computers. You can automate this response with a SEM rule or execute it manually from the Respond menu on the SEM Console.

Requirements

To use this active response, ensure that the file you want to append already exists. Follow these guidelines when creating the file:

- Use a .txt file, or a similar flat-text file format.
- Avoid using spaces in the file path or name.
- Note the complete file path and name, because you will need it to configure the active response.

Configure the Append Text to File active response and Windows active response connectors on each SEM Agent on which you want to be able to use this active response.

Configure the Append Text to a File Active Response connector on a SEM agent

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.

3. Select your agent node, and then click Manage node connectors.
4. In the search box, enter:
append
5. Select the Append Text to File Active Response connector, and then click Add Connector.
6. Enter a new name, or keep the default.
7. From the How to append drop-down list, select Newline to append the text to a new line, or No Newline.
8. Specify a Maximum file size, or accept the default, and then click Add.
9. Under Configured connectors, select your connector, and then click Start.

Configure the Append Text To File action in a rule

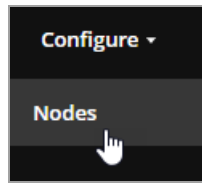
1. Log in to the SEM Console,
2. On toolbar, click Rules.
3. Select an existing rule that triggers on a specific event.
4. Click Edit, and then click Next.
5. Under Actions, click Add new action.
6. Select Append Text to File, and then click Next.
7. Under Define action, begin typing to locate the event defined in your rule definition.
8. Fill in the directory structure in the File Path, indicating the name of the file.
9. The Text field will contain the text that you are inserting into the file. If using plain text, select String from the drop-down list.
10. Click Add, and then click Save.

Configure an active response connector on a SEM agent

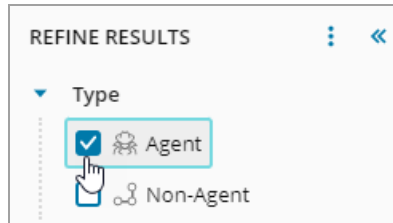
Configure the Windows active response connector on each SEM agent that requires active responses.

You can deploy your SEM agents and configure the Windows active response connector based on where you want to perform these actions. To perform actions at the domain level, deploy a SEM agent to at least one domain controller. To perform actions at the local level, deploy a SEM agent to each computer that requires a response.

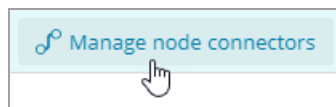
1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.



3. In the Refine Results column, expand Type and select the Agent check box.



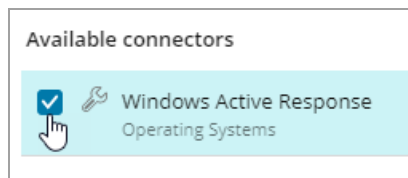
4. Select an agent, and then click Manage node connectors.



5. In the search box, type Windows Active Response and then click the magnifying glass icon.



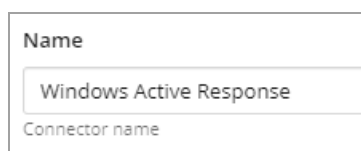
6. Under Available connectors, select the Windows Active Response connector.



7. Click Add Connector.



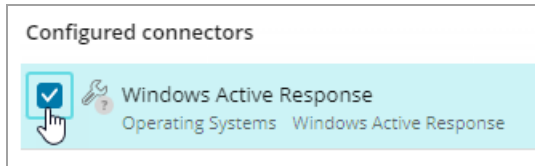
8. Enter a custom alias name for the new connector, or accept the default.



9. Click Add.



10. Under Configured connectors, select your configured connector.



11. Click Start.



The green indicator next to the connector name displays, indicating that the connector is started and running.

Use the Block IP active response in SEM

Use the Block IP active response to block an IP address at your firewall using your SEM Manager. This action is useful for blocking port scanners, and can be automated in a SEM rule, or executed manually from the Respond menu on the SEM Console.

Requirements

You can use the Block IP active response with the following firewalls/modules:

- Cisco PIX
- Cisco ASA
- Cisco Firewall Services Module
- FortiGate Firewalls
- Juniper NetScreen
- Check Point OPSEC
- SonicWALL
- WatchGuard Firebox (including Vclass)

Configure the Active Response connector for one of the firewalls listed above on your SEM manager.

Configure the Active Response connector for your firewall

1. Log in to the SEM Console.
2. On the toolbar click Configure > Manager Connectors.
3. In the search box, enter active response, and then click the magnifying glass icon to begin the search.
4. Select your firewall active response connector, and then click Add Connector.
5. Complete the connector configuration form according to your firewall specifications, and then click Add.
6. Under Configured connectors, select the connector, and then click Start.

Configure the rule

1. Log in to the SEM Console.
2. On the toolbar, click Rules.
3. On the Rules toolbar, click Create new rule.
4. Drag one or more values into the rule definition builder.

The drag panel on the left contains searchable filter values that you can drag into the rule definition builder. Expand a rule values group to select a value, or locate your value by entering a term in the search field.

 When you drag a value into the filter builder, the correct drop location is illuminated with a blue line. [Learn more here.](#)

5. Click Next.
6. Under details and actions, add a descriptive rule name.
7. To add the Active Response tag to your rule, click Add tag, and then select it from the Activity Types list.
8. Click a toggle button to enable the rule after saving, or to enable in test mode.
9. Click Add new action, select Block IP, and then click Next.
10. Enter the IP address to be blocked, click Add, and then click Create.

Block IP active response

The Block IP active response creates a rule on your firewall to block the IP addresses you specify. To allow an IP address through your firewall, delete or modify the rule on your firewall as appropriate.

Configure the Detach USB Device active response in SEM

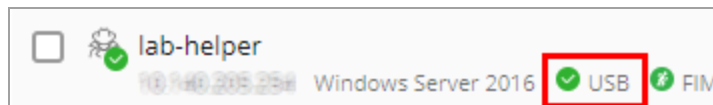
Use the Windows active response to detach a USB device from a SEM agent running USB Defender. This procedure allows only specific devices to be attached to your Windows computers or detach any device exhibiting suspicious behavior. You can automate this procedure in a SEM rule.

USB Defender is an option when the agent is originally installed. If not installed at the time of agent install, re-install the agent with USB Defender. Additionally, configure the Windows Active Response tool on each SEM agent where you require an active response.

Verify that USB Defender is installed on a SEM Agent

1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.
3. In the Refine Results column, expand Type and select the Agent checkbox.
4. Under Refine Results, expand USB Monitoring and select the Installed check box.

The check next to USB indicates USB defender is installed.



If USB Defender is not installed on one or more SEM agents, reinstall the agent and ensure that you select Install USB-Defender after you confirm the Manager Communication Settings.

Detach USB devices

By default, USB devices are audited and the USB File Audit Activity filter will display those events. The filter is set for:

```
FileAuditAlerts.ProviderSID=*USB*
```

To monitor all USB device activity, create a filter for:

```
AnyAlert.ProviderSID=*USB*
```

USB devices are not detached by default. You must configure a rule to detach the device. The SEM Console includes several templates you can access and modify, as shown below.

Create rule from template

Select rule template

Review rule condition

Rule details

Select rule template

↑ Name

usb

☐ Detach USB - Excessive File Copies

USB Device Monitoring

Workstation Monitoring

Server Operations

+9

☐ Detach USB - File Executed

USB Device Monitoring

Workstation Monitoring

Server Operations

+8

☐ Detach USB - Infected Device

USB Device Monitoring

Workstation Monitoring

Server Operations

+7

☐ Detach Unauthorized USB Device

USB Device Monitoring

Workstation Monitoring

Server Operations

+10

☐ USB-Defender Service Stopped

General Best Practice

USB Device Monitoring

Workstation Monitoring

+9

 You can enforce USB Defender policy locally. See [Configure the USB Defender local policy connector](#) for details.

Configure the Disable Networking active response in SEM

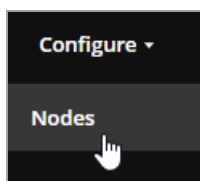
Use the Disable Networking Active Response to disable networking on a SEM agent at the Windows Device Manager level. Use this active response to isolate network infections and attacks. You can automate the active response in a SEM rule or manually execute the response from the Respond menu on the SEM Console.

Use caution with this active response because it responds to the SEM agent at the Device Manager level. To avoid unintentionally disabling networking, consider placing new rules with this action in Test mode until you are sure your correlations are configured appropriately.

Configure the Windows active response connector on each SEM agent that requires active responses.

You can deploy your SEM agents and configure the Windows active response connector based on where you want to perform these actions. To perform actions at the domain level, deploy a SEM agent to at least one domain controller. To perform actions at the local level, deploy a SEM agent to each computer that requires a response.

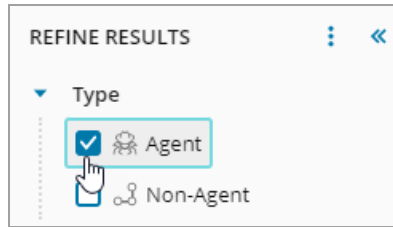
1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.



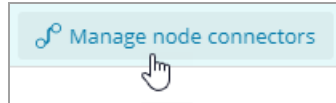
Administrator Guide: Security Event Manager

page 490

3. In the Refine Results column, expand Type and select the Agent check box.



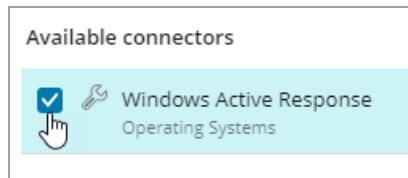
4. Select an agent, and then click Manage node connectors.



5. In the search box, type Windows Active Response and then click the magnifying glass icon.



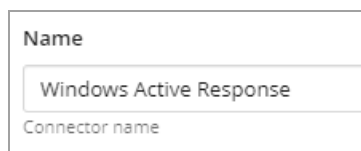
6. Under Available connectors, select the Windows Active Response connector.



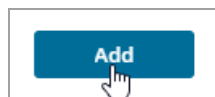
7. Click Add Connector.



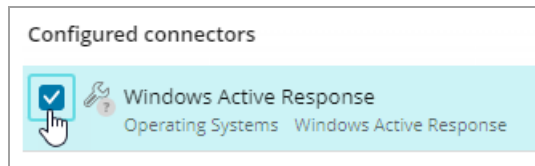
8. Enter a custom alias name for the new connector, or accept the default.



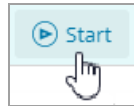
9. Click Add.



10. Under Configured connectors, select your configured connector.



11. Click Start.



The green indicator next to the connector name displays, indicating that the connector is started and running.

Re-enable networking on a computer affected by the active response

1. Log in to the computer locally with administrative privileges.
2. Open Control Panel, and then navigate to System and Security > Administrative Tools > Computer Management.
3. In Computer Management, navigate to System Tools > Device Manager.
4. Expand the Network adapters group.
5. Select the network adapter, and then click Action > Enable.

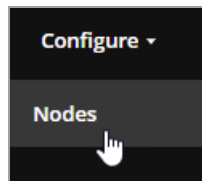
Configure the Kill Process active response in SEM

Use the Kill Process active response to end Windows-based processes in your SEM agents. This response can help you stop suspicious or unauthorized processes running in your network. You can automate the response using a SEM rule or manually execute the response from the Respond menu on the SEM Console.

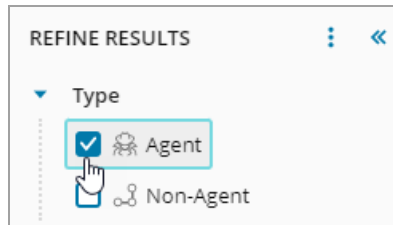
Configure the Windows active response connector on each SEM agent that requires active responses.

You can deploy your SEM agents and configure the Windows active response connector based on where you want to perform these actions. To perform actions at the domain level, deploy a SEM agent to at least one domain controller. To perform actions at the local level, deploy a SEM agent to each computer that requires a response.

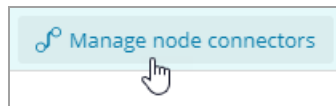
1. Log in to the SEM Console.
2. On the toolbar, click Configure > Nodes.



3. In the Refine Results column, expand Type and select the Agent check box.



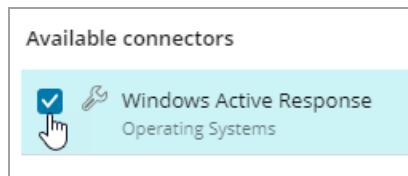
4. Select an agent, and then click Manage node connectors.



5. In the search box, type Windows Active Response and then click the magnifying glass icon.



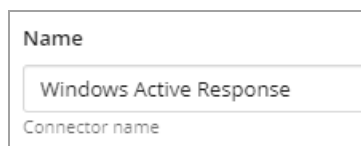
6. Under Available connectors, select the Windows Active Response connector.



7. Click Add Connector.



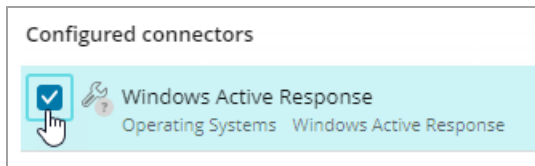
8. Enter a custom alias name for the new connector, or accept the default.



9. Click Add.



10. Under Configured connectors, select your configured connector.



11. Click Start.



The green indicator next to the connector name displays, indicating that the connector is started and running.

Create regulatory and compliance reports

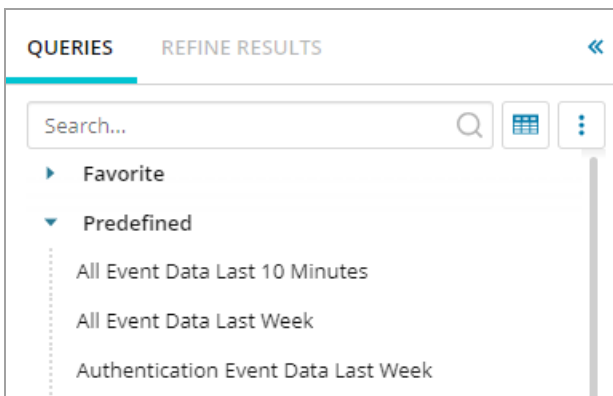
This section describes how to create reports to address your regulatory and compliance requirements.

About SEM reports

The SEM reports convert historical event queries into information you can use to troubleshoot and identify problems in your organization. From within the Historical Events and Reports tab in the toolbar, you can [set up](#) and [run](#) reports on your search queries. These reports help you identify events and trends in your organization, helping you make informed decisions about your network activity.

Predefined queries

In the Historical Events and Reports tab, the Queries tab includes the Predefined category. This category includes several predefined queries included with SEM. You can generate a report for each predefined query. SEM includes several predefined queries that can help you make informed decisions about your network security.



The following table lists the predefined queries included with SEM.

Category	Description
All Event Data Last 10 Minutes	Lists all events that occurred during the last 10 minutes.
All Event Data Last Week	Lists all events that occurred during the previous week.

Category	Description
Authentication Event Data Last Week	Lists all authentications tracked by the SolarWinds system that occurred during the previous week. These authentications include user logon, logoff, failed logon attempts, guest logons, and so on.
Change Management Event Data Last Week	Lists all changes to domains, groups, machine accounts, and user accounts that occurred in the previous week.
Failed Logon Event Data Last week	Lists all Logon Failure events that occurred in the previous week. These events reflect failed account logon events from network devices (including network infrastructure devices).
Firewall Event Data Last Day	Lists all firewall node events that occurred in the previous day.
High Severity Event Data Last Day	Lists all high severity events that occurred in the previous day.
IDS Event Data Last Day	Lists all intrusion detection system (IDS) events that occurred in the previous day.
Incident Event Data Last Day	Lists all incident events that occurred in the previous day.
Incident Event Data Last Week	Lists the Incident, HostIncident, HybridIncident and NetworkIncident events that occurred in the past week. These events reflect enterprise-wide issues.
Network ACL Denied Event Data Last Day	Lists all network access control list (ACL) denied events that occurred in the previous day.
Network Event Data Last Hour	Lists all network events that occurred in the past 60 minutes.
Rule Activity Last Week	Lists all rule activity events that occurred in the past week.

Category	Description
Threat Event Data Last Week	Lists all threat events that occurred in the past week.
Virus Event Data Last Week	Lists all malicious or abusive use of network resources events that occurred in the past week.

Report format

When you run or a SEM report, you can save the report in CSV or PDF format to your system. When you schedule a report, SEM automatically generates the report based on your scheduling settings and sends the report to you or another recipient in a zipped file using your email application.

 All reports are sorted by DetectionTime in descending order--from the latest to the earliest events.

Set up the SEM reports

In version 2023.2.1 and earlier, the SEM Reports application was required to generate reports. Beginning in version 2023.4, you can [run or schedule reports](#) from queries in the Historical Events and Reports tab located in the SEM Console.

To set up the SEM reports engine for the historical event queries:

1. **Set the maximum number of events for the reports.** In the Settings > Event Limits > Report tab, enter the maximum number of events that will be included in your SEM reports. Consider entering a low-to-moderate maximum threshold to consume fewer system resources and maintain optimum SEM performance.

The minimum value is one hundred (100) events. The maximum value is ten million (10000000) events.

2. **Set the maximum email attachment size.** If you plan to send SEM reports to your stakeholders as an email attachment, [set the maximum email attachment size](#) so it conforms with your Microsoft Exchange Server restrictions.

After you set this value, the attachment size restriction displays in the Schedule Search pop-up window when you [schedule a report](#). For example:

 The attachment will not be sent if the size exceeds 999 megabytes. [Change limit](#)

3. **Configure the Email Active Response connector.** To send automated emails to SEM console users when a rule is triggered, [configure the Email Active Response connector](#). This connector specifies the SMTP Relay mail host used to send emails and provides the requisite server credentials.
4. **Set up an email template for the scheduled reports.** Create an email template for all stakeholders who receive the report as an email attachment in a scheduled report. See [Create email templates for use with SEM rules](#) for instructions.
5. **Update the user accounts for all scheduled report recipients.** Ensure that the user accounts of all scheduled report recipients are configured with a valid email address. A valid email is required for all scheduled reports. See [Add SEM users](#) for instructions.
6. **(Optional) Configure an SFTP connection to an external server.** If your reports exceed your email attachment requirements, consider [setting up a secure file transfer protocol \(SFTP\) connection](#) to one or more external Windows or non-Windows systems in your organization. This option allows you to automatically deliver your reports directly to a system in your organization that your stakeholders can access from their systems.

Run or schedule a SEM report

You can run an on-demand report or schedule a report. [On-demand reports](#) are reports you generate when you need them. [Scheduled reports](#) are reports that automatically run on their own based on a specific schedule you set up for each report.

 All reports are sorted by DetectionTime in descending order--from the latest to the earliest events.

These reports are based on the custom and predefined queries in the [Historical Events and Reports](#) tab. When the report is no longer required, you can [unschedule the report](#).

Use these reports as a starting point to [create rules](#) that respond to security events, [monitor and protect specific systems and devices](#) in your network, and [create response actions](#) for your network and system events.

After you run an on-demand report, you can:

- Save the report as a PDF or CSV file.
- Send the report as an email attachment.

 To minimize email errors regarding attachment size, [set the maximum email attachment size setting](#) to notify you when a generated report exceeds the maximum attachment size set by your email provider.

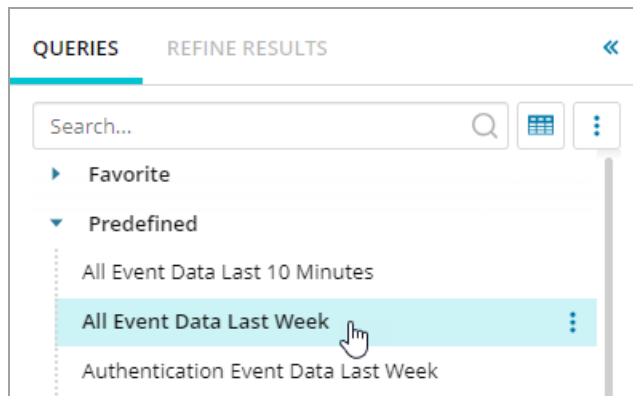
- Send the report to an external server using an [SFTP connection](#).

Run an on-demand report

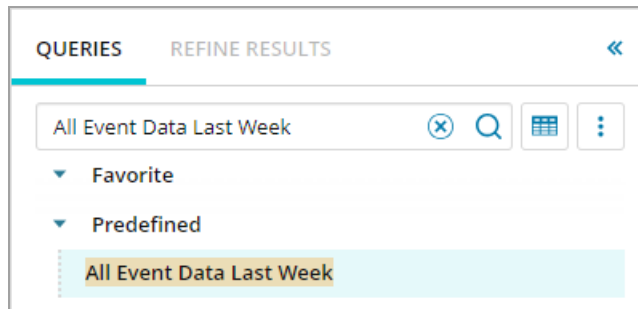
1. Log in to the SEM Console.
2. Click the Historical Events and Reports tab.
3. In the left column, click the Queries tab.



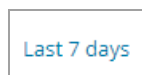
4. Maximize a query category and select a query for the report. For example, All Event Data Last Week.



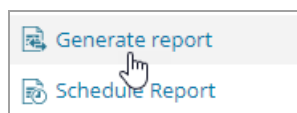
If you know the query name, you can enter the name in the Search field.



After you select a query, the time picker in the toolbar adjusts to the query time range.



5. In the query name, click the vertical ellipsis ⋮ and select Generate report.



 You can also click the Options drop-down menu in the toolbar and click Generate report.

6. In the Name field, enter a name for this report or accept the default name.

Name

All Event Data Last Week

7. In the Format field, select CSV or PDF for the report format.

Format

PDF

PDF

8. If you selected CSV, go to the next step.

If you selected PDF, click the Group by drop-down menu and select an option.

For example, Event Type.

Group by

Event Type

None
Detection IP
Event Type
Provider SID
Tool Alias

9. Click Generate.

A message displays, stating the report progress.

 **Generating report**
Reporting... This might take a few minutes. Do not close this tab.

 Do not close or leave the Historical Events and Reports tab while SEM generates the report.

When the report is completed, the following message displays. The report is added to a ZIP file and downloaded to your system.

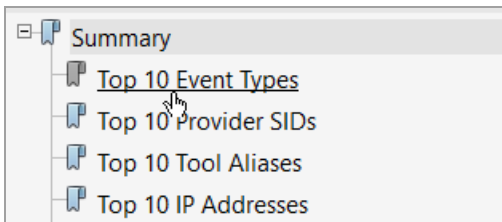
Generating report has finished
Downloading... This might take a few minutes. Do not close this tab.

10. Navigate to the downloaded ZIP file containing the report.
11. Unzip the file using a file archive utility (such as 7-Zip).
12. Double-click the file to open the report.

About the PDF report

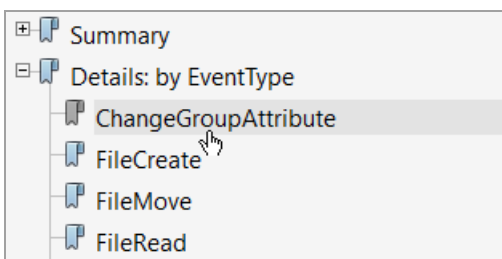
The PDF report groups the reports by Summary and Details. Click the Bookmarks icon  to access all reports in the PDF file.

The Summary reports provide high-level information about the query events in graphical format.

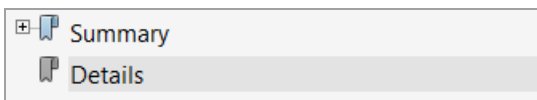


The Detail reports provide in-depth information about the query events in table format. The events are grouped together based on the [Group by option](#) you select for your PDF report.

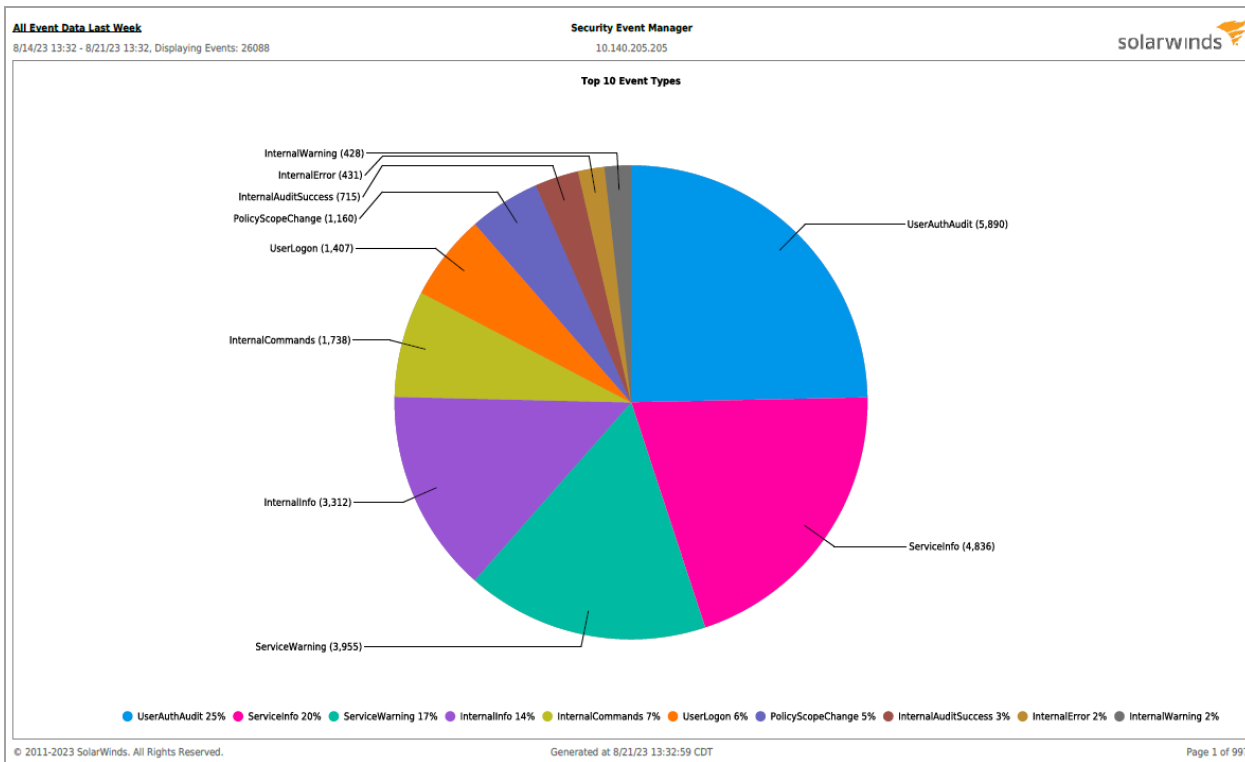
In the following example, the query event data is grouped by the event type. Click an event type to view a report for the selected event type.



If you do not select a [Group by option](#), the query event data for event types is grouped together into one report. Click Details to review the report for all event types.

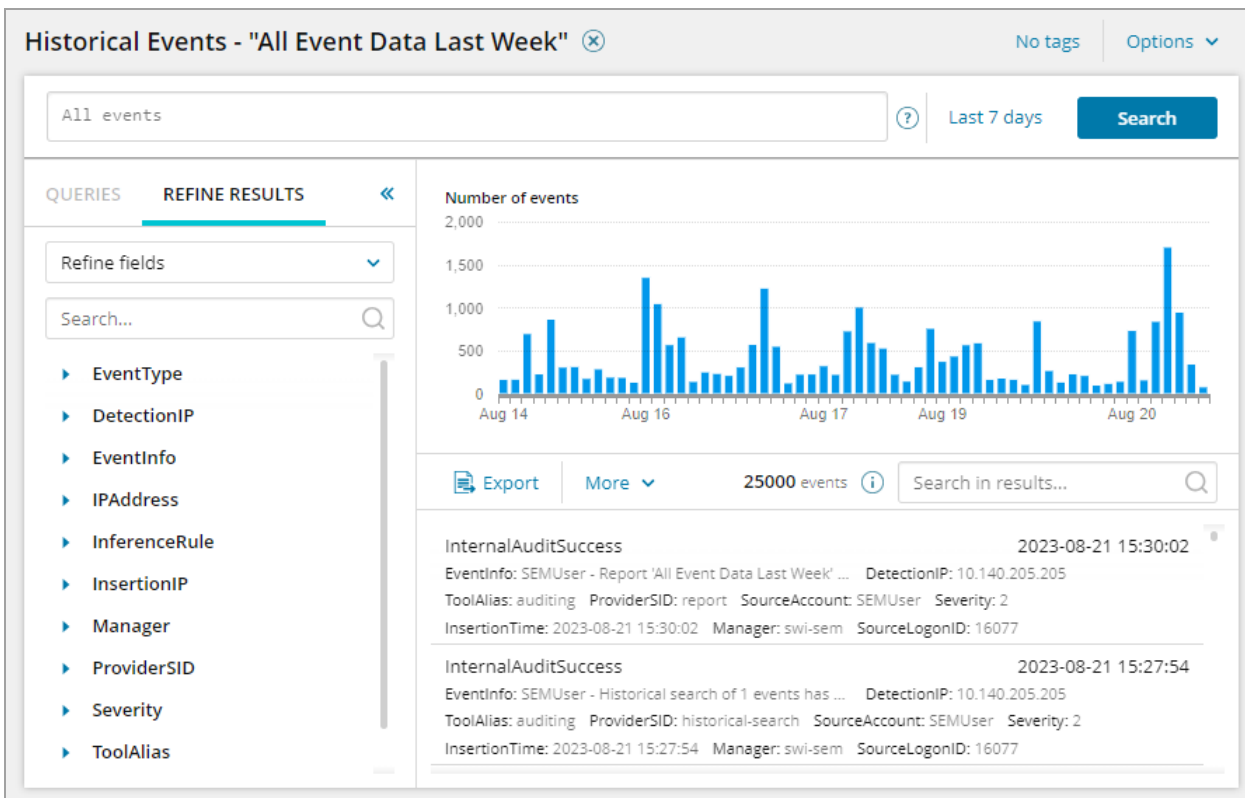


Below is an example of the Top 10 Event Types summary report included in the All Event Data Last Week query.



To return to the query used for your report, click the report name in the top left corner of the report. For example, All Event Data Last Week.

The SEM Console displays the Refine Results tab with a list of all event data associated with the query.

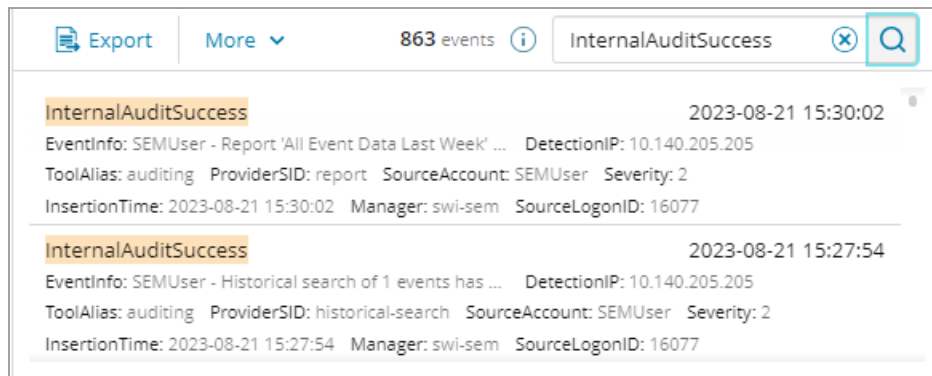


In the Refine Results tab, you can:

- Click Export to export the report data to a CSV file.

 You can import this file into a Microsoft Excel spreadsheet.

- Click More to switch to table view or hide the graph.
- Click  to view the event details and change the historical event limits in the Settings > Event Limits > Historical tab.
- Use the Search field to filter the event list based on your search term. For example:

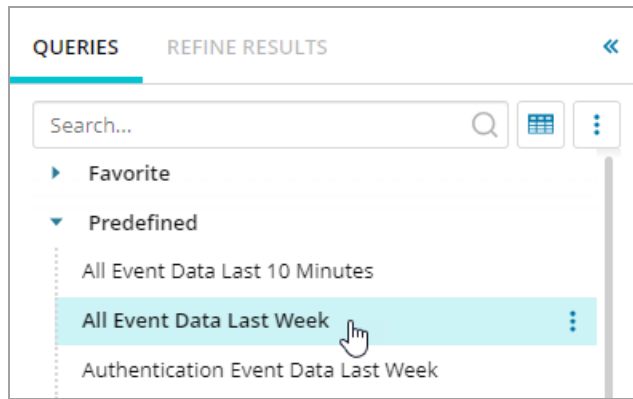


Schedule a report

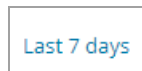
Report schedules automatically email historical event reports to your stakeholders in daily, weekly, or monthly intervals. Use the reports to communicate network trends to your IT security and management personnel. This process can help you respond to network and system events in a timely manner.

1. Create a list of all stakeholders who require performance or status reports on a daily, weekly, or monthly basis.
2. Ensure that your SEM deployment is configured to generate and deliver reports to your stakeholders. See [Set up the SEM reports](#) for instructions.
3. Log in to the SEM Console.
4. Click the Historical Events and Reports tab.
5. In the left column, click the Queries tab.
6. Maximize a query category and select a query for the report.

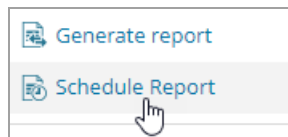
For example, Maximize Predefined and select All Event Data Last Week.



After you select a query, the time picker in the toolbar adjusts to the query time range.



7. Click the vertical ellipsis  and select Schedule report.



 You can also click the Options drop-down menu in the toolbar and click Schedule this query.

8. Under Recurrence Pattern, select a [daily](#), [weekly](#), or [monthly](#) report schedule.

For **daily and custom date reports**, select Daily and the date value in the drop-down menus.

For example, every day...

RECURRENCE PATTERN

Daily

every

1

^

v

day

...or every five days.

RECURRENCE PATTERN

Daily

every

5

^

v

days

For **weekly reports**, select Weekly and the weekly occurrence in the drop-down menus and checkboxes.

For example, every week on Monday and Friday.

For **monthly reports**, select Monthly, the monthly occurrence, and the day or days of the month. For example, every month on the 15th day of the month. Click Add day to add additional days to the schedule.

9. Select an execution time for the report. Click Add time to add one or more execution times.

10. Enter start and end dates for reporting events that occurred on the SEM Manager. The report will only show those events that occurred on the manager within this period.

11. Select a file format for the attached report.

For PDF reports, click Group by and select an option to group the report data. Otherwise, select None.

OPTIONS

Format

PDF

Group by

None

12. Choose the report sharing method. You can share the report as an [email attachment](#) or to an [external server using an SFTP connection](#).

To send the report as an **email attachment**:

- a. Click the Sharing drop-down menu and select Email.

SHARING

Select sharing option

Email

- b. Click the Recipients drop-down menu and select the targeted stakeholders who require this report. Click Add LDAP users to add these users as email recipients, if required.

Recipients

SEMUser (SEMUser@example.com) (x) v

Add LDAP users

- c. Verify that the email template is correct for your email recipients.

Email template: Scheduled Search

To send the report to an external server using an **SFTP connection**:

- a. Click the Sharing drop-down menu and select SFTP.

SHARING

Select sharing option

SFTP

- b. Click the SFTP configuration drop-down menu and select an SFTP connection to an external server.

SFTP

SFTP configuration

Customer Service Reports Server
✕
▼

Manage SFTP

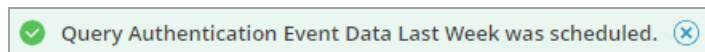
If a connection is not available, click Manage SFTP to [set up a new SFTP connection](#).

- c. Select the checkbox to be notified by email that the report was generated and sent to the stakeholder(s).

☒
Notify via email when the report is done

13. Click Schedule.

A message displays in the console toolbar, stating that the report query is scheduled.

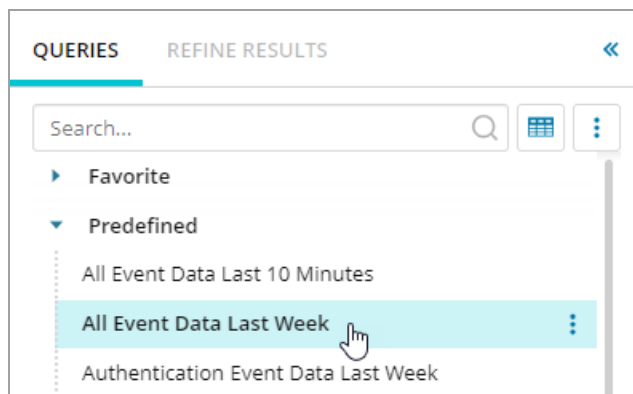


14. Repeat [step 7](#) through step 15 to schedule additional query reports.

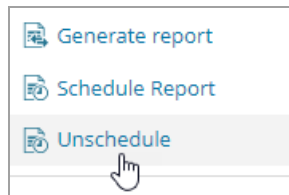
Unschedule a report

1. Log in to the SEM Console.
2. Click the Historical Events and Reports tab.
3. In the left column, click the Queries tab.
4. Maximize a query category and select the query you scheduled for a report.

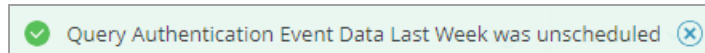
For example, Maximize Predefined and select All Event Data Last Week.



5. Click the vertical ellipsis and select Unschedule.



A message displays in the console toolbar, stating that the report is unscheduled.



Locate migrated SEM audit reports

In version 2023.2.1 and earlier, the SEM Reports application converted SEM database data into on-demand and scheduled audit reports you could use to troubleshoot and identify network problems. Beginning in version 2023.4, you can generate and schedule all reports in the [Historical Events & Reports screen](#).

SolarWinds recommends that you begin creating your on-demand and scheduled reports from within the Historical Events & Reports tab.

In version 2023.4, you can permanently disable the SEM Reports application. See [Disable the SEM Reports application](#) for instructions. The SEM Reports application will be deprecated in a future release.

Locate an audit report query

The following table lists the report queries that were migrated from the SEM Reports application to the SEM web console.

To run a report query, identify the targeted report title and corresponding category or tag name. When you are finished, locate the report by [category](#) or [tag](#) in the web console and run or schedule the report query.

Title	Report	Location
Application Traffic	RPT2003-06-11-5.rpt	Lists all application traffic events.
		Activity Types → Network (tag)
		Compliance → General (tag)

Title	Report		Location
Attack Behavior: Access	RPT2003-11.rpt	Shows malicious asset access through the network. For example, attacks on FTP or Windows Network servers, malicious network database access, abuses of services, or attempted unauthorized entry.	Activity Types → Network (tag) Compliance → Healthcare (tag), Compliance → Education (tag) Compliance → General (tag)
Attack Behavior: Denial / Relay	RPT2003-12.rpt	Tracks activity associated with network denial or relay attack behaviors. This report shows malicious asset relay attempts and denials of service through the network. For example, FTP bouncing, Distributed Denial of Service events, and many protocol abuses.	Activity Types → Network (tag) Compliance → Healthcare (tag), Compliance → Education (tag) Compliance → General (tag)
Authentication	RPT2003-02.rpt	Lists all authentications tracked by the SolarWinds system, including user logon, logoff, failed logon attempts, guest logons, and so on.	Compliance → Healthcare (tag) Compliance → Education (tag) Compliance → General (tag)

Title	Report		Location
Authentication: Log On / Off/ Failure	RPT2003-03.rpt	Tracks activity associated with account events such as log on, log off and log on failures.	Compliance → Healthcare (tag)
		This is a refined version of the Authentication Report that does not include SolarWinds authentication events. It is more appropriate for management reports or audit reviews than regular use.	Compliance → Education (tag)
			Compliance → General (tag)
Core Traffic	RPT2003-06-11-5.rpt	Lists all core traffic events.	Activity Types → Network (tag)
			Compliance → General (tag)
File Audit Event	RPT2003-05.rpt	Tracks file system activity associated with audited files and system objects, such as file access successes and failures.	Compliance → Healthcare (tag)
			Compliance → Education (tag)
			Compliance → General (tag)
File System Audit	RPT2003-09-010.rpt	Tracks activity associated with file system audit events including mount file system and unmount file system events.	Compliance → General (tag)
		These events are generally normal system activity, especially during system boot.	

Title	Report	Location
General Authentication: Domain Events	RPT2006-20-01.rpt	Includes changes to domains, including new domains, new members, and modifications to domain settings. Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)
General Authentication: Group Events	RPT2006-20-02.rpt	Lists changes to groups, including new groups, members added/removed to/from groups, and modifications to group settings. Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)

Title	Report		Location
General Authentication: Machine Account Events	RPT2006-20-03.rpt	Includes changes to machine accounts, including enabling/disabling machine accounts and modifications to machine account settings.	Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)
General Authentication: User Account Events	RPT2006-20-04.rpt	Includes changes to user accounts, including enabling/disabling user accounts and modifications to user account settings.	Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)

Title	Report		Location
Malicious Code	RPT2003-04.rpt	Tracks event activity associated with malicious code such as virus, Trojans, and worms, both on the network and on local machines, as detected by anti-virus software.	Compliance → Healthcare (tag) Compliance → Education (tag) Compliance → General (tag)
Network Infrastructure Policy/View Change	RPT2006-21.rpt	Includes accesses to network infrastructure device policy, including viewing or changing device policy.	Change Management → Policy changes (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)
Process Audit	RPT2003-09-030.rpt	Tracks activity related to processes, including processes that have started, stopped, or reported useful process-related information.	Compliance → General (tag)

Title	Report		Location
Registry Audit Events	RPT2003-05-75.rpt	Lists registry audit events.	Compliance → Healthcare (tag)
	RPT2003-05-76.rpt		
	RPT2003-05-77.rpt		Compliance → Education (tag)
	RPT2003-05-78.rpt		
	RPT2003-05-79.rpt		Compliance → General (tag)
	RPT2003-05-80.rpt		
	RPT2003-05-81.rpt		
	RPT2003-05-82.rpt		
	RPT2003-05-83.rpt		
	RPT2003-05-84.rpt		
	RPT2003-05-85.rpt		
	RPT2003-05-86.rpt		
Resource Configuration	RPT2003-08.rpt	Details events that relate to configuration of user accounts, machine accounts, groups, policies and their relationships	Compliance → Federal (tag)
			Compliance → Healthcare (tag)
			Compliance → Education (tag)
			Compliance → General (tag)
Service Audit	RPT2003-09-040.rpt	Tracks activity related to services, including services that have started, stopped, or reported useful service-related information or warnings.	Compliance → General (tag)

Title	Report		Location
SolarWinds Actions	RPT2003-18.rpt	Lists all commands or actions initiated by SolarWinds Network Security.	Compliance → Federal (tag) Compliance → Healthcare (tag) Compliance → Education (tag) Compliance → General (tag)
Suspicious Behavior	RPT2003-07.rpt	Tracks activity associated with suspicious network behaviors such as reconnaissance or unusual traffic. Specifically, this report shows potentially dangerous activity, such as excessive authentication failures, port scans, stack fingerprinting, and network enumerations.	Compliance → Federal (tag) Compliance → Healthcare (tag) Compliance → Education (tag) Compliance → General (tag) Activity Types → Network (tag)
System Audit	PT2003-09-020.rpt	Tracks activity associated with system status and modifications, including software changes, system reboots, and system shutdowns.	Compliance → General (tag)
USB Defender	RPT2003-09-050.rpt	Tracks activity associated with USB-Defender, including insertion and removal events related to USB Mass Storage devices.	Compliance → General (tag)

Title	Report		Location
Web URL Requests	RPT2003-06-01-5.rpt	Lists the most frequently visited URLs grouped by the requesting client source machine.	Activity Types → Network (tag) Compliance → Healthcare (tag) Compliance → Education (tag) Compliance → General (tag)
Windows/Active Directory Domains: Group Events	RPT2006-22.rpt	Includes Windows/Active Directory group-related events.	Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)

Title	Report		Location
Windows/Active Directory Domains: Machine Events	RPT2006-23.rpt	Includes Windows/Active Directory machine-related events.	Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)
Windows/Active Directory Domains: New Critical Group Members	RPT2006-22-04.rpt	Includes additions of Windows/Active Directory user accounts to critical groups, such as Domain or Enterprise Admins.	Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)

Title	Report		Location
Windows/Active Directory Domains: OU Events	RPT2006-24.rpt	Includes Windows/Active Directory Organizational Unit-related events.	Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)
Windows/Active Directory Domains: User Events	RPT2006-25.rpt	Includes Windows/Active Directory user-related events.	Change Management → General Best Practice (tag) Compliance → Education (tag) Compliance → Federal (tag) Compliance → General (tag) Compliance → Healthcare (tag)

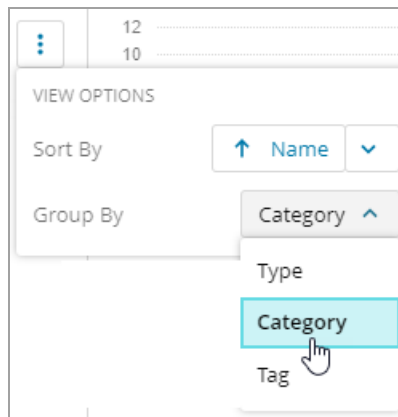
Locate a report by category

This procedure describes how to locate a report by category—for example, the Application Traffic report.

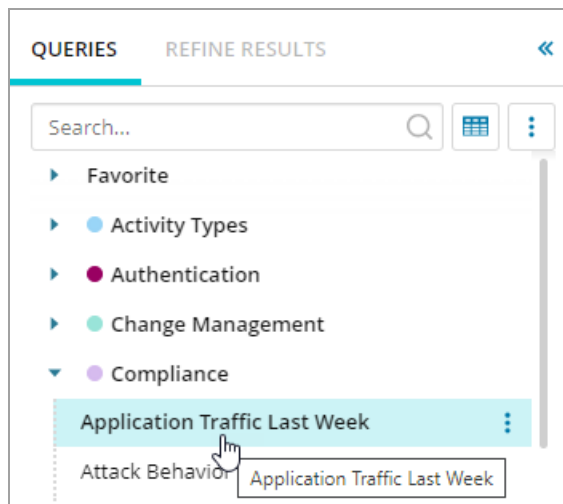
1. Log in to the SEM Console.
2. Click the Historical Events & Reports tab.
3. In the left column, click the Queries tab.



4. Click the vertical ellipsis and select Group By Category.



5. In the [Default audit report locations table](#), locate the Application Traffic report.
6. In the Category column select a category. For example, Compliance.
7. In the left column, expand the Compliance query menu.
8. Locate and click the targeted report.



9. Run or schedule the report.

See [Run or schedule the report](#) for instructions.

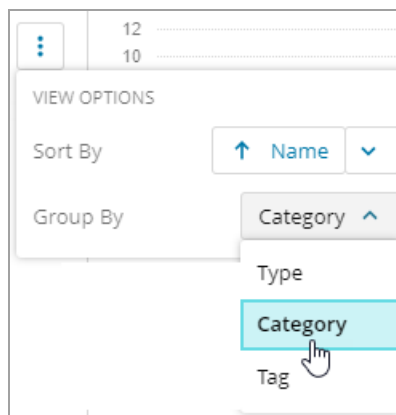
Locate a report by tag

This procedure describes how to locate a report by tag—for example, the Application Traffic report.

1. Log in to the SEM Console.
2. Click the Historical Events & Reports tab.
3. In the left column, click the Queries tab.

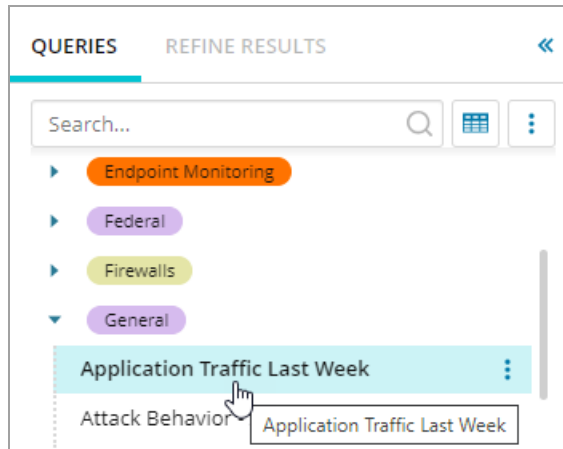


4. Click the vertical ellipsis and select Group By Category.



5. In the [Default audit report locations table](#), locate the Application Traffic report.
6. In the Tag column select a tag. For example, General.

7. In the left column, expand the General tag menu.
8. Locate and click the targeted report.



9. Run or schedule the report.

See [Run or schedule the report](#) for instructions.

Disable the SEM Reports application

Perform the following steps to disable the SEM Reports application.

1. [Log in to the CMC command-line interface.](#)
2. Access the [CMC service menu.](#)

At the command prompt, execute:

```
service
```

3. At the `cmc::service>` prompt, execute:

```
restrictreports
```

4. When prompted for an IP address, execute:

```
127.0.0.1
```

The SEM Reports application is disabled.

About the CMC

This section provides information on how to use the command-line interface (CLI) to perform routine administrative tasks on a SEM virtual machine (VM).

About the CMC command line

The CMC provides a command-line interface (CLI) for performing routine administrative tasks on a SEM VM.

 See [Log in to the SEM CMC command line interface](#) for login steps and information about credentials and SSH access restrictions.

Use CMC commands for tasks such as:

- Upgrading the Manager software
- Manually applying connector updates
- Deploying new connector infrastructure to the Managers and Agents
- Rebooting or shutting down the network appliance
- Configuring trusted reporting hosts
- Configuring supplemental services on the Manager appliance

Special characters allowed in CMC commands and passwords

The following table lists the special characters you can use in your CMC commands and passwords.

Character	Example
Capital letters	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Lower-case letters	abcdefghijklmnopqrstuvwxyz
Numerals	0123456789
Symbols	<code>_ ` ~ ! @ # \$ % ^ & * () - = + ' [{] } \ ; : a " A , 1 < . > / ?</code>
White spaces	<code>command1 command2 command3</code>

The CMC main menu opens when you log in to the CMC command-line interface.



See [About the CMC command line in SEM](#) for information about using the CMC command line.

Commands are listed in order of appearance.

Command	Description
appliance	Displays the <code>appliance</code> menu to run network and system commands on the SEM VM. You can activate the VM, configure network parameters, and change the CMC password. See SEM CMC appliance menu for more information.
manager	Displays the <code>manager</code> menu where you can run upgrade and debug commands on the SEM Manager. You can install a SEM hotfix, start and stop the SEM Manager service, and import a certificate used for desktop console communication. See SEM CMC manager menu for more information.

Command	Description
service	Displays the <code>service</code> menu to run restrictions and SSH. You can start and stop the SSH Service and restrict access to the reports application by IP address or host name. See SEM CMC service menu for more information.
rawlogs	Displays the <code>rawlogs</code> menu to run configuration and maintenance commands.
upgrade	Installs the SEM upgrade package that you will use to upgrade your SEM VM. This command functions the same as the <code>hotfix</code> command.
admin	Opens the admin command-line interface in the Lynx text browser.
import	Imports a keytab file from Active Directory into SEM. This file is required to configure SEM for Active Directory single sign-on. See Set up single sign-on (SSO) in SEM for details.
help	Displays the Help menu.
exit	Exits the CMC management console.

CMC appliance menu

The `cmc::appliance>` menu includes commands for managing network and system settings.

 See [About the CMC command line in SEM](#) for information about using the CMC command line.

Type the `appliance` command at the main menu to open the `cmc::appliance>` prompt. Commands available from the appliance menu are listed in the following table in alphabetical order.

Y in the "Restart Required" column indicates that a command requires an automatic restart of the SEM Manager service. See [Start and stop the SEM appliance and agent](#) for help.

Command	Description	Restart Required
activate	Configures essential SEM features. Run this command after you install the SEM license. See Run the activate command to secure SEM and configure network settings for instructions.	N
checklogs	Shows the contents of the SEM log files from sources such as syslog and SNMP.	N

Command	Description	Restart Required
<code>clearsyslog</code>	Removes all rotated and compressed local files.	N
<code>cleantemp</code>	Removes temporary files SEM created during normal operation. Run this command to recover used disk space, or at the suggestion of SolarWinds Support.	N
<code>dateconfig</code>	Sets/shows the SEM VM's date and time.	N
<code>dbdiskconfig</code>	Configures the database retention setting (that is, the percentage of free space for the database). This command requires an automatic restart of the SEM Manager service.	Y
<code>diskusage</code>	Checks disk usage consumed by the SEM Manager and several other internal components (such as the database or log files), and provides a summary. This information is included when you send SolarWinds Support information using the <code>support</code> command.	N
<code>diskusageconfig</code>	Sets the SEM Manager disk usage limit by the percentage of unavailable disk space or the amount of free disk space.	N
<code>editbanner</code>	Edits the SSH login banner.	N
<code>exit</code>	Exits the <code>appliance</code> menu and returns to the main menu.	N
<code>exportsyslog</code>	Exports the system logs.	N
<code>hostname</code>	Changes the hostname of the SEM VM.	N
<code>import</code>	Imports the SIM or SEM backup to the SEM.	N
<code>limitsyslog</code>	Interrogates and/or changes the number of rotated log files to be kept.	N
<code>multimanagerconfig</code>	Enables or disables the multimanager.  If you enable multimanager, some security scanners may generate cross-domain security warnings about SEM. If this feature is not required, keep it disabled.	N
<code>setlogrotate</code>	Sets the syslog rotation frequency to either hourly or daily.	N
<code>netconfig</code>	Configures network settings for the SEM VM, such as the IP address, subnet mask, and DNS server(s).	N

Command	Description	Restart Required
ntpconfig	Configures the Network Time Protocol (NTP) service on the SEM VM for synchronization with a time server.	N
password	Changes the CMC user password.	N
ping	Pings other IP addresses or host names from the SEM VM to verify network connectivity.	N
reboot	Reboots the SEM VM.	N
shutdown	Shuts down the SEM VM.	N
top	Displays and monitors CPU and memory usage, as well as per process information for the Manager Network Appliance.	N
tzconfig	Configure the SEM VM time zone information.	N
viewnetconfig	Displays the SEM VM network settings, such as the IP address, subnet mask, and DNS server(s).	N
exit	Exits the <code>appliance</code> menu and returns to the main menu.	N

CMC manager menu

The `cmc::manager>` menu includes commands for upgrading and debugging SEM.

 See [About the CMC command line in SEM](#) for information about using the CMC command line.

Type the `manager` command at the main menu to open the `cmc::manager>` prompt. Commands available from the manager menu are listed in the following table in alphabetical order. Y in the Restart Required column indicates a command requires an automatic restart of the SEM Manager service. See [Start and stop the SEM appliance and agent](#) for help.

Command	Description	Restart Required?
archiveconfig	Configures the SEM Manager appliance database archives to a remote file share on a daily, weekly, or monthly schedule.	N

Command	Description	Restart Required?
<code>backupconfig</code>	Configures the SEM Manager appliance software and configuration backups to a remote file share on a daily, weekly, or monthly schedule.	N
<code>cleanagentconfig</code>	Reconfigures the Agent on the current SEM Manager instance to connect to a new SEM Manager.	N
<code>confselfsignedcert</code>	Configures the SEM Manager to use a server.	N
<code>dbrestart</code>	Restarts the database.	N
debug	Sends debugging information from the SEM Manager to any given email address. The email message contains a collection of data that can be useful in diagnosing problems.	N
exit	Exits the <code>manager</code> menu and returns to the main menu.	N
exportcert	Exports the CA certificate so that you can import it into a computer running the SEM console.	N
exportcertrequest	Exports the SEM Manager certificate (along with its public and private key) so that your certificate authority (CA) can sign it using PKI tools.	N
<code>hotfix</code>	Installs a SEM hotfix. This command functions the same as the <code>upgrade</code> command.	N
importcert	Imports a certificate signed by any certificate authority (CA). A certificate is required to encrypt communication with the SEM console.	Y
<code>importl4ca</code>	Imports a CA of the other node in an L4 configuration.	Y
<code>licenseupgrade</code>	Upgrades your SEM Manager license.	Y
logbackupconfig	Configures the Manager appliance remote log backups to a remote file share on a daily, weekly, or monthly schedule.	N

Command	Description	Restart Required?
resetadmin	Resets the admin password to <i>password</i> . This command does not affect other users on the system, and all settings are preserved.	Y
restart	Restarts the SEM Manager service. This will take the Manager offline for 1–3 minutes.	Y
sensortoolupgrade	Upgrades the SEM Manager's Sensor Tools from the command line. This command does not support cd rom and floppy options - only SB.	N
showlog	Allows you to page through the SEM Manager's log file.	N
showmanagemem	Displays the SEM Manager's configured memory utilization settings.	N
start	Starts the SEM Manager service. If the Manager is already started, then nothing will happen.	N
stop	Stops the SEM Manager service. This makes the Manager inactive until it is started again.	Y
support	This command has been deprecated. Use the debug command.	N
viewsysinfo	Displays appliance settings and other information that is useful for support and troubleshooting.	N
watchlog	Displays 20 lines of the current SEM Manager log file and monitors the log for further updates. Any new log entries appear as they are written to the log.	N

CMC service menu

The `cmc::service>` menu includes commands for managing restrictions and SSH access.

 See [About the CMC command line in SEM](#) for information about using the CMC command line.

Type the `service` command at the main menu to open the `cmc::service>` prompt. Commands available from the service menu are listed in the following table in alphabetical order. Y in the "Restart Required" column indicates that a command requires an automatic restart of the SEM Manager service. See [Start and stop the SEM appliance and agent](#) for help.

Command	Description	Restart Required
<code>disableflow</code>	Disables the flow Collection Service on the appliance (and in the SolarWinds Explorer).	N
<code>enableflow</code>	Enables the flow Collection Service on the appliance (and in the SolarWinds Explorer).	Y
<code>exit</code>	Exits the <code>service</code> menu and returns to the main menu.	N
<code>help</code>	Displays a brief description of each command within the <code>service</code> menu.	N
<code>restartssh</code>	Restarts the SSH service. If the SSH service is running, this command stops and then restarts the service.	N
<code>restrictconsole</code>	Restricts access to the SEM console to only certain IP addresses or hostnames. This command prompts you to provide the IP addresses or hostnames that should be allowed access. Once the restriction is in place, only the listed IP addresses or hostnames can connect to the SEM console. Also see <code>unrestrictconsole</code>.	N
<code>restrictreports</code>	Restricts access to reports to only certain IP addresses or hostnames. This command prompts you to provide the IP addresses or hostnames that should be allowed access. Once the restriction is in place, only the listed IP addresses or hostnames can create and view reports. Also see <code>unrestrictreports</code>.	N
<code>restrictssh</code>	Restrict the SSH service to only certain IP addresses. This command prompts you to provide the IP addresses that should be allowed access. Once the restriction is in place, only the listed IP address and user combinations can connect to the SEM Manager using the SSH service. Also see <code>unrestrictssh</code>.	N

Command	Description	Restart Required
snmp	Configures the SNMP Services. See Enable the SNMP Trap Logging Service in SEM to configure SEM to receive SNMP traps. See Set up SEM to communicate with NPM and the SolarWinds Platform Web Console using SNMP to configure SEM and NPM to monitor SEM's CPU, memory, and other critical components.	N
startssh	Starts the SSH service.	N
stopopsec	Terminates any connections from the SEM Manager VM to Check Point® Open Platform for Security (OPSEC) hosts.	N
stopssh	Stops the SSH service. If you issue this command, you can only access the SEM Manager with a keyboard and monitor until you issue a <code>reboot</code> command. To restrict access to the SSH service (outside of the user name and password requirements), see the <code>restrictssh</code> command.	N
unrestrictconsole	Removes access restrictions placed on the SEM console. The only remaining protection is the user name and password combination. This command removes all other restrictions and allows system users with a user name and password to connect to the console.	N
unrestrictssh	Removes access restrictions placed on the SSH service. The only remaining protection is the user name and password combination	N

CMC rawlogs menu

 See [About the CMC command line in SEM](#) for information about using the CMC command line.

Type the `rawlogs` command at the main menu to open the `cmc : rawlogs>` prompt. Commands available from the rawlogs menu are listed in the following table in alphabetical order. Y in the "Restart Required" column indicates that a command requires an automatic restart of the SEM Manager service. See [Start and stop the SEM appliance and agent](#) for help.

Command	Description	Restart Required
<code>configurerawlogs</code>	Configure the manager to use a Raw logs service.	Y
<code>logmarchiveconfig</code>	Sets the raw logs archive share settings.	N
<code>logmbackupconfig</code>	Sets the raw logs backup share settings.	N
<code>restart</code>	Restarts the raw logs search/storage service.	Y
<code>showsearchanges</code>	Displays search ranges per search core	N
<code>start</code>	Starts the raw logs search/storage service.	N
<code>stop</code>	Stops the raw logs search/storage service.	N
<code>exit</code>	Exits the <code>rawlogs</code> menu and returns to the main menu.	N

Troubleshoot your SEM deployment

This section describes how to troubleshoot and resolve issues in your SEM deployment.

See the following Knowledge Base (KB) articles for additional troubleshooting information.

- [SEM reboot for troubleshooting](#)
- [Troubleshoot Network Devices Logging to SEM](#)
- [Startup errors display after increasing the SEM disk size](#)

Troubleshoot alerts in the SEM Console

This section describes how to troubleshoot unmatched data or internal new connector data alerts that may appear in your SEM console.

Typically, unmatched data and internal new connector data alerts indicate that one or more of the connectors on the SEM VM or appliance cannot properly normalize the associated log data.

1. Ensure that your syslog devices are sending logs to a syslog facility on your SEM appliance.
2. Determine which devices are logging to each facility, and whether those devices conflict with each another.
3. Ensure that your SEM Agent connectors, such as Windows-based and database connectors are running correctly.
4. Apply the latest connector update package.
5. Generate a syslog sample from the SEM appliance, and then [open a ticket](#) with SolarWinds Technical Support for further assistance.

Task 1: Troubleshoot syslog devices

Complete the following troubleshooting procedures for devices that send logs to a syslog facility on your SEM appliance.

1. Verify that the connector and device are pointed at the same local facility.
2. Check the configuration on your device to determine what local facility it is logging to on your SEM appliance. In some cases, you cannot modify this setting.

 For additional information, search for your device in the [SolarWinds Success Center](#). Except for CheckPoint firewall, the SEM receives UDP syslog data on port 514.

3. Verify that the connector is pointed to the same logging facility as the device.
 - a. On the SEM Console, navigate to Configure > Manager Connectors.
 - b. Under Configured connectors, locate the connector in the list.
 - c. Select the configured connector, and then click Edit.
 - d. View its details, and verify the Log File value matches the output value in the device configuration.
4. If the device and connector configurations do not match, point the connector to the appropriate location.
 - a. Select the configured connector, and then click Stop.
 - b. Click Edit, and then change the Log File value so it matches your device.
 - c. Click Save, and then click Start.

Task 2: Troubleshoot device logging

Certain devices (including Cisco devices) have similar logging formats that cause connector conflicts when logging to the same facility on your SEM appliance. Use the following procedure and table to determine what devices are logging to each facility, and whether those devices conflict with one another.

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

2. At the `cmc>` prompt, type `appliance`.
3. At the `cmc::appliance>` prompt, type `checklogs`.
4. Enter an item number to select and view a local facility.
5. To view the device sending the event, open the log facility.

The `EPOCH timestamp (1427722392000)` starts each event, which is the date and time in Unix numeric format. The device sending the event follows. You will typically see `ProviderSID (ASA-1-106021)`, which is similar to an Event ID.

6. If two or more devices are logging to the same facility, see [Troubleshoot conflicting devices" below](#) to determine whether those devices conflict with each other.

Troubleshoot conflicting devices

Different firewall types should log to different facilities. For example, Cisco firewalls and Palo Alto should log to different facilities.

However, both devices should log to their own facilities. Ensure that the devices in each of these groups are logging to distinct local facilities on your SEM VM. For example, if a device in Group 1 is logging to `local1`, make sure a device in Group 2 is not also logging to that facility.

i SolarWinds recommends splitting the devices and vendors to different facilities. Having all devices pointed at one facility with multiple connectors reading that facility will impact your SEM performance.

Group	Devices
Group 1	Cisco ASA
	Cisco IOS
	Cisco PIX
Group 2	Cisco Catalyst (CatOS)
Group 3	Cisco Wireless LAN Controller (WLC)
Group 4	Cisco Nexus
Group 5	Cisco VPN
Group 6	Dell PowerConnect

Task 3: Troubleshoot Agent devices and connectors

Complete the following steps to troubleshoot SEM Agent connectors, such as Windows-based and database connectors.

1. Verify the connector is pointing to the appropriate folder or event log.
2. Check the configuration on the host computer to determine which folder or event log it is logging in to.

In some cases, you cannot modify this setting. For additional information, search the [SolarWinds Success Center](#) for your device.

3. Verify that the connector is pointed to the same folder or event log as the device:
 - a. On the SEM Console, navigate to Configure > Nodes.
 - b. Under Refine Results, expand the Type group, and then select the Agent check box.
 - c. Select the SEM Agent for the host computer, and then click Manage node connectors.
 - d. Locate the configured connector in the list.

- e. Select the configured connector, and then click edit.
 - f. View its details, and ensure the Log File value matches the output value in the host computer configuration.
4. If the host computer and connector configurations do not match, point the connector to the appropriate location:
 - a. Select the configured connector, and then click Stop.
 - b. Click Edit, and then change the Log File value so it matches your device.
 - c. Click Save, and then click Start.

Task 4: Apply the latest connector update package

If you completed the procedures in this section and you still see the unmatched data or internal new connector data alerts, apply the latest connector package before you contact Technical Support.

See [Apply a SEM connector update package](#) to learn how.

Task 5: Contact SolarWinds Technical Support

If you are unable to resolve your issue using this article, [open a ticket](#) with SolarWinds Technical Support for further assistance. Be prepared to provide the following information to a support technician:

- A copy of the SEM report (in Crystal Reports format) entitled Tool Maintenance by Alias for the last 24 hours or the period during that the unmatched data was detected.
- (Syslog devices only). A sample of the logs currently sent to SEM for the affected connector. For more information, see [Export log files using the CMC exportsyslog command](#).
- (Windows connectors only). A copy of the entire event log in English and EVTX formats.
- (Database connectors only). A sample of the event table containing the unread events and the details about these events.
- (Database connectors only). The database schema (if available).

Generate a syslog sample from the SEM appliance

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

2. At the `cmc>` prompt, type `appliance`.
3. At the `cmc::appliance>` prompt, type `exportsyslog`.
4. Enter an item number to select a local facility to export.

5. Repeat the previous step to specify more than one facility.
6. Enter `q` to proceed.
7. Follow the on-screen instructions to complete the export.

Troubleshoot SEM agents and network devices

If you do not see the events you expected to see on the SEM Console, use the following procedures to troubleshoot your SEM Agents and network devices.

Determine if SEM is receiving data from a device

SolarWinds recommends starting with this task before moving on to the other troubleshooting tasks.

1. Open the CMD command line.

See [Log in to the SEM CMC command line interface](#) for directions.

2. At the `cmc>` prompt, enter:

```
appliance
```

3. At the `cmc::appliance>` prompt, type:

```
checklogs
```

4. To select a local facility to view, enter an item number.
5. Search for the specific device logging to this facility (such as the product name, device name, or IP address).

See also:

- [Troubleshoot devices not logging to a log file " below](#)
- [Troubleshoot devices logging to a log file " on the facing page](#)

Troubleshoot devices not logging to a log file

Perform the following procedure for network devices that do not show data on the SEM appliance.

1. Ensure that the device is configured to log to the SEM appliance.
2. Ensure that the device is logging to the correct IP address for the SEM appliance.
3. If the device sends SNMP traps to the SEM appliance, ensure that the SEM Manager is configured to accept SNMP traps.

See [Enable SEM to receive SNMP traps](#) for details.

4. Ensure that a firewall is not blocking data communications between the device and the SEM appliance.

Troubleshoot devices logging to a log file

Perform the following procedure for network devices that display data in SEM.

1. Ensure that the appropriate connector is configured on the SEM appliance.
2. Ensure that your configured connector is running.
3. If the connector is running, delete and recreate the connector instance.

Troubleshoot a SEM Agent

To begin, ensure that the SEM Agent is connected to the SEM appliance:

1. On the SEM Console, navigate to Configure > Nodes.
2. Under Refine Results, expand the type group, and then select the Agent check box.
3. In the Status column, note the status icon for the SEM Agent:
 - If the SEM Agent does not appear in the Nodes list, see [Troubleshoot a missing SEM Agent](#).
 - If the SEM Agent appears in the Nodes list with a `Connected` status , see [Troubleshoot a connected SEM Agent](#).
 - If the SEM Agent appears in the Nodes list with a `Disconnected` status , see [Troubleshoot a disconnected SEM Agent](#).

See also:

- [Troubleshoot SEM Agent connections, 64-bit](#) in the SolarWinds Customer Success Center
- [Troubleshoot SEM Agent connections, 32-bit](#) in the SolarWinds Customer Success Center

Troubleshoot a missing SEM Agent

1. Verify that the SEM Agent is installed on the host computer.
2. Verify that the SEM Agent service is running on the host computer.

Troubleshoot a disconnected SEM Agent

1. On the host computer, verify that the SEM Agent Service is running.

If the service is not running, start the service.

If the service is running, go to the next step.

2. On the host computer, ping the SEM VM or appliance by hostname.

If the ping is successful, clear the SEM Agent certificate.

If the ping is not successful, go to the next step.

3. On the host computer, ping the SEM VM or appliance by IP address.

If the ping is successful, the SEM Agent is connected. See ["Troubleshoot a connected SEM Agent" on the next page](#).

If the ping is not successful:

- a. Resolve any network or firewall issues between the SEM Agent and the SEM VM/appliance.
- b. Change your DNS settings so the SEM Agent computer can resolve the SEM appliance hostname (recommended).
- c. Edit or delete the `spop.conf` file (based on your system bit type) so that the SEM Agent calls the SEM VM or appliance by its IP address instead of its hostname.

See ["Edit or delete the spop.conf file " on the next page](#).

Edit or delete the spop.conf file

Perform the following procedure so the SEM Agent calls the SEM appliance by its IP address (Windows systems only).

1. Stop the SolarWinds Security Event Manager Agent service.
2. If you are running a 32-bit Windows system, delete the `spop` folder. Do not delete the `ContegoSPOP` folder.

The folder is located at:

`C:\Windows\System32\ContegoSPOP\spop`

If you are running a 64-bit Windows system:

- a. Open the following directory:

`C:\Windows\SysWOW64\ContegoSPOP\spop`

- b. Open the `spop.conf` file in a text editor.
- c. Replace the `ManagerAddress` value with the SEM appliance IP address.
- d. Save and close the file.

3. Start the SolarWinds Security Event Manager Agent service.

Troubleshoot a connected SEM Agent

1. Verify that you configured the appropriate connectors on the SEM Agent.

For example, the SEM agent for Windows runs the connectors for the Windows Application and Security Logs by default. However, you must configure the connector for the DNS server role.

2. Verify that all configured connectors are running properly.
3. If all configured connectors are running properly, delete and recreate the non-working connectors.

Contact SolarWinds Customer Support

If events from your network device do not appear on the SEM Console after completing these procedures, send a screen shot of the device logging configuration screens and the appropriate system files to [SolarWinds Customer Support](#).

If you are running a 32-bit Windows system, send the following files to SolarWinds Customer Support:

- `C:\Windows\System32\ContegoSPOP\spoplog.txt` (the most recent version)
- `C:\Windows\System32\ContegoSPOP\tools\readerState.xml`

If you are running a 64-bit Windows system, send the following files to SolarWinds Customer Support:

- `C:\Windows\SysWOW64\ContegoSPOP\spoplog.txt` (the most recent version)
- `C:\Windows\SysWOW64\ContegoSPOP\tools\readerState.xml`

Troubleshoot network and syslog device logging in SEM

 If a No Device Found error message appears in the widget, make sure that you configured the device to send logs to the correct IP address. See [Troubleshoot alerts on the SEM Console](#) for troubleshooting steps.

SEM console does not display syslog data

Verify that your devices are configured to forward syslog data to the SEM virtual appliance IP address. If your appliance cannot receive logs, your device may not be supported.

If your devices are configured correctly and your SEM appliance is still not receiving syslog data, identify the facilities that are collecting log data. When you complete this process, configure the appropriate connector from the facility to the log device so Security Event Manager can normalize and monitor this information in the SEM Manager.

Identify your syslog data facilities containing log data

Verify that Security Event Manager is receiving the raw data from your syslog devices.

 See your hypervisor documentation for information about using the virtual console.

1. Open the CMC command line.

See [Log in to the SEM CMC command line interface](#) for directions.

2. At the `cmc>` prompt, type `Appliance`.

```

////////////////////////////////////
///      SolarWinds Security Event Manager      ///
///                               management console                               ///
////////////////////////////////////

Detected VMware Virtual Platform
Product Support Key: 
Available commands:
[ appliance ] Network, System
[ manager ]   Upgrade, Debug
[ service ]   Restrictions, SSH
[ rawlogs ]   Raw logs Configuration/Maintenance
upgrade       Upgrade this Appliance
help          display this help
exit          Exit
cmc >

```

3. At the `cmc::appliance>` prompt, type `checklogs` and press Enter.

The appliance displays all facilities receiving logs from syslog devices, such as firewalls, routers, and switches.


```

Available log files:
[1]: Syslog Log (4.0K)
[2]: SNMP Trap Log (Empty)
[3]: Snort Alert Log (Empty)
[4]: Auth Log (12K)
[5]: Daemon Log (Empty)
[6]: User Log (Empty)
[7]: Solr Log (4.0K)
[8]: Database Log (Empty)
[9]: Manager Configuration Log (12K)
[10]: Kernel Log (Empty)
[11]: Migration log (Empty)
[12]: Syslog local0 Log (4.0K)
[13]: Syslog local1 Log (Empty)
[14]: Syslog local2 Log (208K)
[15]: Syslog local3 Log (Empty)
[16]: Syslog local4 Log (Empty)
[17]: Syslog local5 Log (62M)
[18]: Syslog local6 Log (1.1M)
[19]: Syslog local7 Log (Empty)
Choose a log to view and press enter (1-19, q to quit):

```

In this example, 1, 12, and 18 are active syslog facilities because they contain stored log data. Facilities 13, 15, 16, and 17 are inactive because their syslog log files are empty.

4. Match a facility with a monitored device.

- Choose a facility number and record the local number (such as `local2`) for a future step.
- Enter your chosen facility number (for example, 14 for `local2`), and then press Enter.
- Enter `b` or `E` to view the beginning or end of the log file, respectively, and press Enter.
- Enter the number of lines to display on your screen, and then press Enter.

 Pressing Enter defaults the output to 500 lines.

- Press Enter again.

The raw data appears on your screen.

- Review and match the data to a monitored syslog device in your network.

5. Repeat steps 3 and 4 in this section to match additional facilities with log data to a monitored syslog device in your network.

Syslog Facility	Log File Path
local0	/var/log/local0.log
local1	/var/log/local1.log
local2	/var/log/local2.log
local3	/var/log/local3.log

Syslog Facility	Log File Path
local4	/var/log/local4.log
local5	/var/log/local5.log
local6	/var/log/local6.log
local7	/var/log/local7.log

Glossary of SEM terms

Active response: An action that you or a SEM rule can take in response to suspicious activity or an attack. Active response actions include the *Block IP active response*, the *Disable Networking active response*, the *Log off User active response*, the *Kill Process active response*, the *Detach USB Device active response*, and so on.

Actor: A connector sub-type that can perform an active response. The actor connector allows the Agent to receive instructions from the SEM Manager and perform active responses locally on the Agent computer, for example, sending pop-up messages or detaching USB devices. On the SEM Console, an orange connector icon represents an actor connector. Also see *sensor*.

Agent: In SEM, a software application that collects and normalizes log data before it is sent to the SEM Manager. The Agent runs as a standalone service and provides additional event alerting on workstations and servers. An Agent is required for some active responses, including logging off a user, shutting down a computer, and detaching a USB device. SEM Agents use Secure Socket Layer/Transport Layer Security (SSL/TLS) to securely transmit log data. Also see *connector*.

Agent node: In SEM, a single Agent, syslog, or SMTP instance that sends events to SEM. For example, an environment with 10 routers, 50 switches, 5 firewalls, 300 servers, and 500 workstations has 865 nodes sending data to SEM Manager.

Alert: See [event](#).

Appliance: Originally, SEM was sold as a physical appliance that you deployed on your network. Today, SEM is the virtual image of a Linux-based appliance.

CMC: A command-line interface you can use to interact with the SEM Manager VM to perform routine administrative tasks without root access.

Connector: In SEM, a connector is a stand-alone file that allows SEM to monitor and interact with third-party vendor products, for example a firewall, an anti-virus application, a router, and so on. Each connector is named after the specific product that it is designed to support. Connectors can reside either on a SEM Agent, or on the SEM VM. Connectors installed on an Agent monitor local log files, but they can also monitor events sent from remote devices that cannot run an Agent. Connectors can intercept syslog events sent by third-party network devices and translate them into normalized events. Whereas SEM Agents actively send normalized log events to the SEM Manager, connectors rely on the host system to send syslog events to the SEM Manager. Connectors have two subtypes: sensors and actors. A *sensor* retrieves data from the product that the connector supports, whereas an *actor* carries out active responses.

Correlation: See [event correlation](#).

Directory service group: In SEM, directory service groups are Windows users and computer accounts that SEM pulls from Active Directory. You can associate directory service groups with rules and filters. Use directory service groups if Active Directory is available so that you do not have to manually update lists of user and computer accounts in user-defined groups.

Event: Any alert or notification written to a log that is monitored by SEM. In SEM, the terms *event* and *alert* are interchangeable.

Event correlation: The process of extracting useful and/or significant information from the large number of events flowing in to SEM. Event correlation works by looking for and analyzing relationships between different event sources.

Event distribution policy: SEM's event distribution policy controls how events are routed through the system. By configuring the event distribution policy, you can disable (or exclude) specific event types at the event level from being sent to the SEM console and/or the SEM database. Use the event distribution policy to prevent events of little or no value from being processed by the console or stored in the database.

Event group: A group type used to organize events for use with rules and filters. If you use an event group in a rule, SEM fires the rule when any event in the group triggers an alert.

Event response: See [active response](#).

Facility code: A numeric code specified by the syslog protocol to identify the type of program that is logging the message. Sixteen facility codes, ranging from 0 (kernel messages) to 15 (clock daemon), are reserved for known program types, whereas facility codes 16 through 23 are reserved for local use (local use 0 up to local use 7). In SEM, facility codes are used to route vendor-specific events to designated log files.

Filters: Filters capture events and alerts that take place on your network. Filter conditions can be broad or specific. For example, you can create a filter without conditions that captures all events, regardless of the source or event type, or you can create a filter that has one specific condition, such as UserLogon Exists, which only captures user logon events. SEM ships with filters that support best practices in the security industry. You can modify these filters to meet your needs.

Filter groups: Also called *filter categories*. Filter categories are used to organize *filters* in SEM. SEM installs with seven default categories in the Filters pane: Overview, Security, IT Operations, Change Management, Authentication, Endpoint Monitoring, and Compliance. Administrators can remove or rename these categories, or add new categories as needed.

File Integrity Monitoring: Also called *FIM*. A SEM feature that monitors system and user file activity to protect sensitive information from theft, loss, and malware. FIM detects changes to critical files and registry keys to ensure that they are not accessed or modified by unauthorized users. FIM ensures systems comply with regulatory regulations, including Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Sarbanes-Oxley. FIM is enabled either by adding a FIM connector to a node, or by adding FIM to an existing connector profile.

Flat file log: Any log output to one or more ASCII-based text files. Systems that write to flat file logs include Linux system logs, web server logs, DNS server logs, custom application logs, and others.

Groups: In SEM, groups organize related elements into logical units so that they can be used in rules and filters. Various group types are used to group events, data elements (such as IP addresses, user names, web site URLs, and so on), Active Directory users and computers, email templates, Agents and connectors, and time-of-day sets.

Hypervisor: Computer software that runs virtual machines. The SEM VM can be installed on two hypervisors: Microsoft Hyper-V Server, and VMware vSphere ESX 4.0 or ESXi 4.0 and later.

SEM Manager: The SEM component that collects and processes log messages sent by one or more network systems. The SEM Manager consists of a syslog server, an optimized database, a web server, a correlation engine, and a hardened Linux operating system. SEM Manager is deployed as a single VM to a hypervisor (either Hyper-V or vSphere) running on Windows Server.

Local Agent Installer: A standalone installer that you or another administrator runs on a local host system to install the SEM Agent. The Local Agent Installer can be used for attended or unattended SEM Agent installations. Also see *Remote Agent Installer*.

Manager: See [SEM Manager](#).

NCR: An initialism for *New Connector Request*. An NCR is a request for SolarWinds to create a connector for a system or application that does not have one.

NCD: An initialism for *New Connector Data*. An NCD is a request for SolarWinds to update an existing connector to receive data that is either being missed or is coming in as unmatched.

Node: An *Agent* instance monitored by SEM. On the SEM Console, navigate to Configure > Nodes to display the Agents monitored by each of your SEM Managers.

Normalization: The process by which SEM translates raw log data into a standard format prior to storing the message in the database. The SEM Manager component and the SEM Agent component are both capable of normalizing raw event messages received from devices on a network.

Ops Center: See [Ops Center view](#).

Ops Center view: In the web console, the user interface view that provides a dashboard made up of multiple widgets to help identify trends and problem areas in the network. Administrators can customize the dashboard by adding, editing, and removing widgets.

raw log retention: The raw log retention component in SEM is a separate data store to which you can send raw (unnormalized) log messages. The database is an optional component that is disabled by default. To save raw log messages, you need to enable it.

Remote Agent Installer: A standalone installer that pushes SEM Agents to Microsoft Windows hosts across your network without the need to step through an installation wizard. The installer unzips the installation files to a temporary folder of your choice, searches for Windows systems across the network, and installs the SEM Agent one at a time to the targeted systems. Also see *Local Agent Installer*.

Roles: SEM uses roles to restrict user access to sensitive data. Each SEM user account must be assigned to one of six SEM role types: *Administrator*, *Auditor*, *Monitor*, *Contact*, *Guest*, and *Reports*.

Rules: Rules monitor event traffic and automatically respond to events in real time. When an event (or a series of events) meets a rule condition, the rule prompts the SEM Manager to carry out a response action. A response action can be discreet, such as sending notifications to the appropriate users by email; or it can be active, for example blocking an IP address or stopping a process.

Sensor: A connector sub-type that cannot perform an active response. On the SEM Console, a blue connector icon represents a sensor connector. See also *actor*.

Severity: In the syslog protocol, severity is a numeric code used to specify the urgency of the notification. Severity ranges from 0 (emergency: system is unusable) to 7 (debug: debug-level messages).

SIEM: A category of software products and services that monitor and analyze security events generated by applications and hardware devices on a network and send notifications when a set threshold is reached. Security Event Manager (SEM) is a fully-featured SIEM solution. SIEM is an initialism for *security information and event management*.

Single sign-on: SEM supports Active Directory single sign-on (SSO). When enabled, SEM does not request a user name and password if the user is already logged in to Active Directory (AD). Instead, AD authenticates the user in the background, and automatically logs the user in to SEM with the appropriate user access rights.

SNMP, SNMP monitoring: Simple Network Management Protocol is used to collect information from network devices. SEM can receive SNMP traps from SolarWinds solutions to correlate performance alerts with SEM events. SEM can also send SNMP traps to SolarWinds solutions to enable NPM to monitor CPU, memory, and other critical SEM components.

SSO: See [single sign-on](#).

Syslog: A message logging protocol used by a wide range of devices, including most network devices, such as routers, switches, and firewalls. Devices send event notification messages to a central logging server (a syslog server) that consolidates logs from multiple sources. Syslog messages have a numeric facility code that SEM uses to route messages to a log. to specify the type of program that is logging the message, and a numeric severity level to specify the urgency of the notification.

Syslog server: A software application (such as Kiwi Syslog Server) that collects syslog messages and SNMP traps from network devices (such as routers, switches, and firewalls).

USB defender: A free add-on for all SEM Agents installed on Windows computers. USB defender tracks events related to USB mass storage devices like flash drives and smart phones, and allows the SEM Manager to send commands to detach offending devices both manually and automatically.

User-defined group: User-defined groups are groups of data elements that can be used in rules and filters to match, include, or exclude events, information, and data fields. Data elements can be IP addresses, user names, email addresses, web site URLs, and so on.

Virtual appliance: A type of virtual machine that hosts a single application on a *hypervisor*. To keep things simple, the SEM documentation refers to the SEM virtual appliance as the SEM *virtual machine* (or the *SEM VM*). The SEM virtual appliance runs on a hardened, Linux-based software stack that includes a database, a web server, a correlation engine, a syslog server and a SNMP trap receiver.

vSphere: A *hypervisor* distributed by VMware. The SEM virtual machine can be deployed on vSphere.

Widget: A user interface component that provides special dashboard functionality, such as displaying real-time information about network activity, or providing tools for investigating events and related details.