



GETTING STARTED 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

Get started with SolarWinds Security Event Manager	4
Tasks to help you started with SEM	5
Log in to the SEM Console	6
Determine which logs to monitor with SEM	7
Configure your devices to send events to SEM	9
About syslog local facilities	9
Verify that events are being sent to SEM	10
Configure a SEM agent	13
Install a Windows agent	13
Configure the agent	14
Add a syslog device to SEM	17
Navigate the SEM Console	19
Dashboard	19
Live Events	20
Historical Events & Reports	21
Rules	21
Nodes	22
Configuration	23
User-defined groups and email templates	23
Beyond Getting Started with SEM	25
SEM Getting Started: Additional Resources	26

Get started with SolarWinds Security Event Manager

This guide is for SolarWinds customers who have purchased or want to evaluate SolarWinds Security Event Manager (SEM).

If you are interested in evaluating SolarWinds SEM, you can [download the product](#), fully-functional for 30 days. After the evaluation period, you can convert your evaluation license to a production license by obtaining and applying a license key.

This guide will help familiarize you with the commonly used features of SEM so you can begin detecting suspicious activity, mitigate security threats, achieve auditable compliance, and maintain continuous security.

If you are a customer and need implementation help, search the [SolarWinds Customer Success Center](#) or contact our [Support Team](#). See [SolarWinds Customer Support](#) for details on opening a support case.

If you are evaluating this product and need assistance, [contact SolarWinds Sales](#).

Tasks to help you started with SEM

Complete the following tasks to get started with SEM:

☐ [Log in to the SEM Console](#)

Log in to the console to perform your tasks.

☐ [Determine which logs to monitor in SEM](#)

Decide which logs you want to monitor. If you monitor too many logs, working on the SEM Console can be overwhelming.

☐ [Configure the audit policy on your device to send events to SEM](#)

Only events that you have designated to be sent to SEM are visible on the SEM Console.

☐ [Verify that events are being sent to SEM](#)

Learn how to use the SEM Contego Management Console (CMC) to verify that syslog event data is being sent to SEM.

☐ [Configure an agent in SEM](#)

Learn how to add your first Microsoft Windows computer to SEM.

☐ [Add a syslog device to SEM](#)

Learn how to add a Cisco Adaptive Security Appliance (ASA) firewall to SEM.

☐ [Navigate the SEM Console](#)

After SEM is receiving log data, use the SEM Console to search, view, and filter the data.

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:

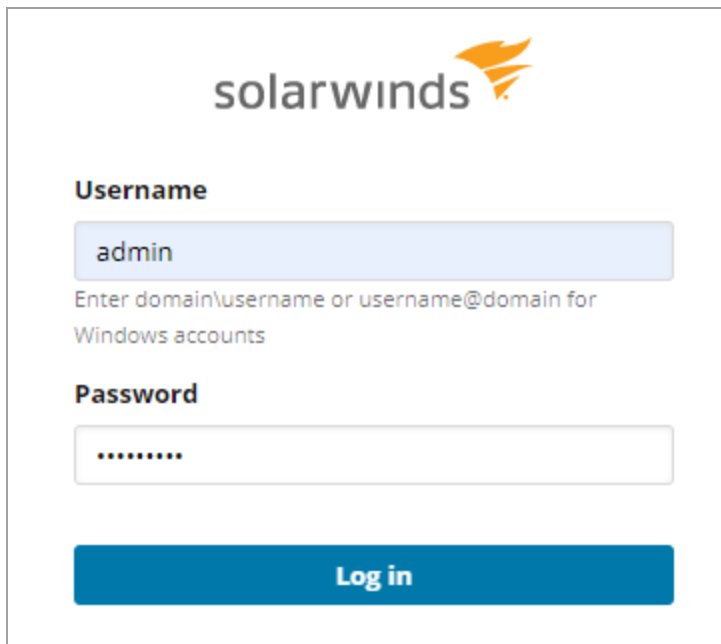
`https://<appliance-ip-or-hostname>`

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 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.

Determine which logs to monitor with SEM

Before you begin monitoring logs with SEM, SolarWinds recommends that you decide which logs to monitor. Avoid an everything, all at once approach, as it is easy to become overwhelmed when all log data is sent to SEM. To determine which logs to monitor, do the following.

1. **Identify your goals by listing what you want to accomplish with your log data.** Consider the business drivers that require you to monitor logs.

If you have a compliance-related goal, you could focus on your data center and monitor security events. If your goal is to monitor logs for outages, you could verify that your servers are sending logs, and that you are receiving events from Microsoft Windows event logs.

2. **Identify the systems that have the log data you want to monitor.** If your goal is to monitor logs so you are PCI-compliant, identify the systems and network devices that are in scope for compliance.

For each identified system and network device, identify which specific logs are in scope, and the level of logging, if applicable.

3. **Begin with what you know.** This can help you avoid learning about SEM and your logs at the same time.

Monitor the logs that are familiar, and then scale from there. For example, if you are most familiar with your Windows security, application, and system event logs, begin monitoring those logs first. SEM also provides connectors to read many other different types of logs.

Use the following table to identify the logs to collect:

If You Need To Track...	Collect These Kinds Of Logs
Changes	User/Groups: Windows security logs Systems: Windows system and application logs Application-specific logs Network devices (firewalls, routers, switches, etc): syslogs
Authentication failures and successes	Windows security logs Application-specific logs Authentication logs on other platforms

If You Need To Track...	Collect These Kinds Of Logs
Internal and external unexpected network activity	Proxy server logs Network device logs (syslog)
Service and system activity	Windows systems logs Application logs
Compliance	Core operating system logs Application logs

Configure your devices to send events to SEM

After you [determine the types of log files to monitor with SEM](#), ensure that your devices are configured to send log data to SEM.

The application does not automatically scan your environment for network devices and systems and collect and analyze log files. You must configure the identified devices and systems to send log data of interest. When you are finished, add those devices to SEM.

If you observe SEM collecting seemingly meaningless data or no data at all, do the following:

1. [Determine which logs are important for you to monitor.](#)
2. Verify that the targeted devices and systems are configured to send that data.

The following graphic shows a section of a sample audit policy for a workstation. If you are expecting Plug and Play events to be written to the log file and the policy is set to No Auditing, then those events are not sent to SEM.

Detailed Tracking	
Process Creation	Success and Failure
Process Termination	Success and Failure
DPAPI Activity	No Auditing
RPC Events	No Auditing
Plug and Play Events	No Auditing

See [Integrate Cisco network devices with SolarWinds SEM](#) for details on how to add a syslog device to SEM. See [Add a syslog device to SEM](#) for details on how to configure the corresponding connector.

For additional guidance, see your vendor documentation or [contact SolarWinds Technical Support](#).

See [Audit Policies and Best Practices for SEM](#) for more information on Windows audit policies.

About syslog local facilities

When you configure the events and logging level on a syslog device, you may have the option to specify the local facility that receives the log data. While all syslog devices have default facilities defined for logs, the option to specify the local facility depends on the device.

Check with the device vendor for details on how to configure your network device. Note the local facility, as you will need it when you configure a connector to read the applicable syslog file. If you are not sure which local facility is receiving log data, check your device.

See [Understanding syslog in SEM](#) for more information on configuring your syslog device to send log data to SEM.

Verify that events are being sent to SEM

After you [configure your device to send events to SEM](#), use the check logs tool to verify that SEM is receiving the data.

You can access the SEM command line using VMware vSphere or Microsoft HyperV Manager virtualization consoles. You can also use an SSH tool to verify that the raw syslog data is received by the SEM syslog server.

 Raw syslog data is not yet parsed or normalized by SEM.

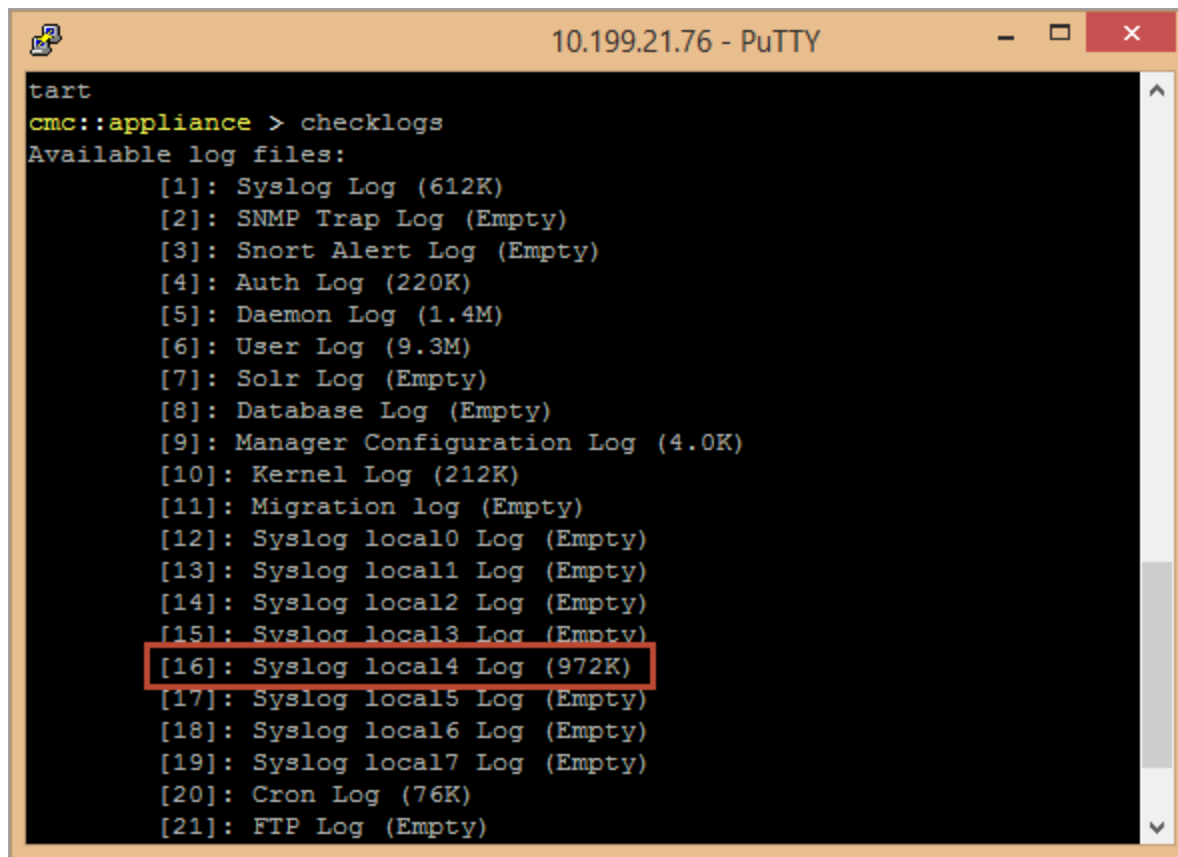
The following example shows how to use PuTTY to verify that SEM is receiving events.

1. Open an SSH tool (such as PuTTY).
2. Enter the IP address and port number (port 22) of the SEM virtual appliance.
3. Log in with username `cmc`.

If you are using a SEM evaluation copy, enter `password` as the password.

4. Open the appliance menu and run the `checklogs` command.
5. Determine which local facilities are receiving traffic.

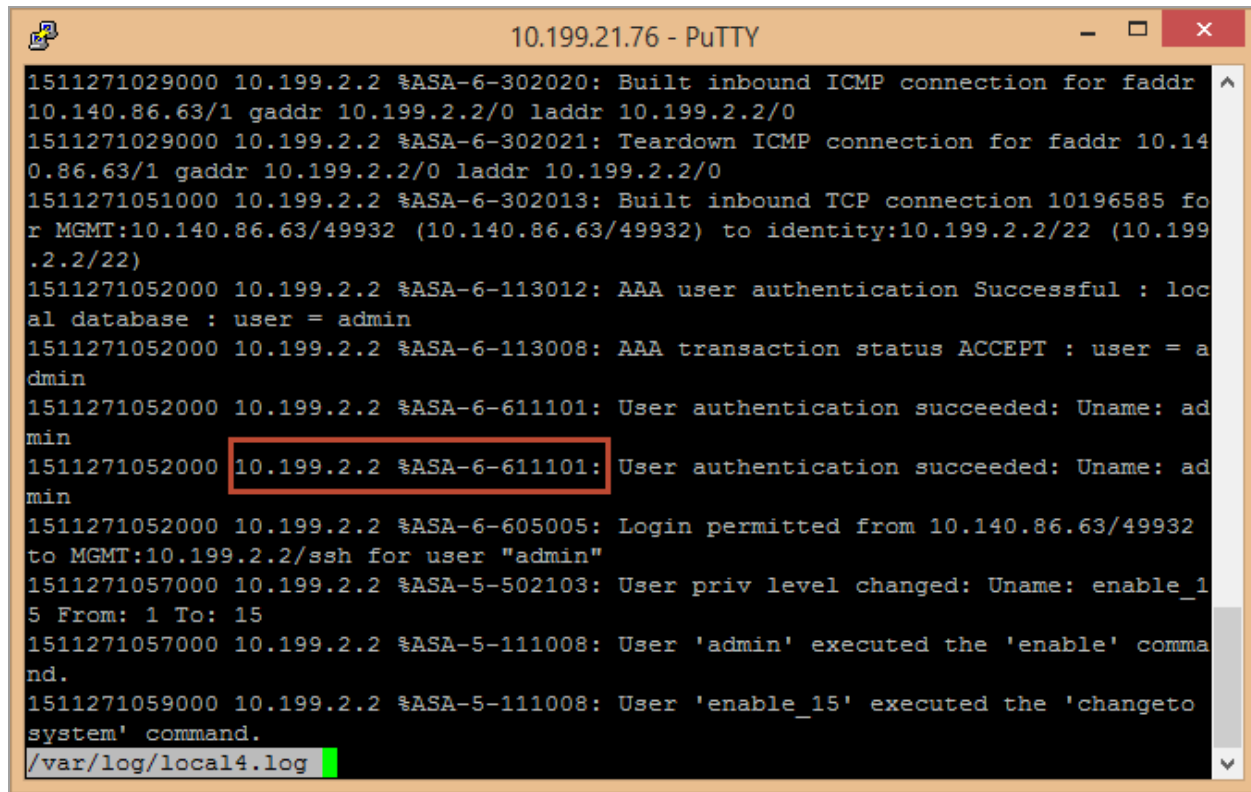
In the following example, local facility 4 has received 972 kilobytes of traffic while all other facilities are empty.



```
tart
cmc::appliance > checklogs
Available log files:
[1]: Syslog Log (612K)
[2]: SNMP Trap Log (Empty)
[3]: Snort Alert Log (Empty)
[4]: Auth Log (220K)
[5]: Daemon Log (1.4M)
[6]: User Log (9.3M)
[7]: Solr Log (Empty)
[8]: Database Log (Empty)
[9]: Manager Configuration Log (4.0K)
[10]: Kernel Log (212K)
[11]: Migration log (Empty)
[12]: Syslog local0 Log (Empty)
[13]: Syslog local1 Log (Empty)
[14]: Syslog local2 Log (Empty)
[15]: Syslog local3 Log (Empty)
[16]: Syslog local4 Log (972K)
[17]: Syslog local5 Log (Empty)
[18]: Syslog local6 Log (Empty)
[19]: Syslog local7 Log (Empty)
[20]: Cron Log (76K)
[21]: FTP Log (Empty)
```

6. Open the local facility to determine if it is receiving the logs you are expecting.

In the following example, local facility 4 is receiving traffic from the Cisco ASA firewall that was configured to send logs.



```

1511271029000 10.199.2.2 %ASA-6-302020: Built inbound ICMP connection for faddr
10.140.86.63/1 gaddr 10.199.2.2/0 laddr 10.199.2.2/0
1511271029000 10.199.2.2 %ASA-6-302021: Teardown ICMP connection for faddr 10.14
0.86.63/1 gaddr 10.199.2.2/0 laddr 10.199.2.2/0
1511271051000 10.199.2.2 %ASA-6-302013: Built inbound TCP connection 10196585 fo
r MGMT:10.140.86.63/49932 (10.140.86.63/49932) to identity:10.199.2.2/22 (10.199
.2.2/22)
1511271052000 10.199.2.2 %ASA-6-113012: AAA user authentication Successful : loc
al database : user = admin
1511271052000 10.199.2.2 %ASA-6-113008: AAA transaction status ACCEPT : user = a
dmin
1511271052000 10.199.2.2 %ASA-6-611101: User authentication succeeded: Uname: ad
min
1511271052000 10.199.2.2 %ASA-6-611101: User authentication succeeded: Uname: ad
min
1511271052000 10.199.2.2 %ASA-6-605005: Login permitted from 10.140.86.63/49932
to MGMT:10.199.2.2/ssh for user "admin"
1511271057000 10.199.2.2 %ASA-5-502103: User priv level changed: Uname: enable_1
5 From: 1 To: 15
1511271057000 10.199.2.2 %ASA-5-111008: User 'admin' executed the 'enable' comma
nd.
1511271059000 10.199.2.2 %ASA-5-111008: User 'enable_15' executed the 'changeto
system' command.
/var/log/local4.log

```

If you are not seeing the log data that you expect to see:

- Check the network device vendor documentation for instructions on configuring your device.
- See [How to Troubleshoot Syslog Nodes in SolarWinds Security Event Manager](#) for guidance on troubleshooting situations when SEM is not receiving log data.

Configure a SEM agent

For non-network devices, you can install a SEM agent on workstations and servers to collect and normalize log data before it is sent to SEM.

The SEM agent also collects security data from each device (such as Windows event logs and database logs) and transmits this data to SEM. The agent creates a small footprint on the device and prevents log tampering during data collection and transmission.

Using the SEM agent, you can:

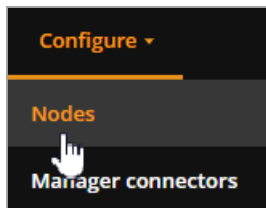
- Capture events in real-time
- Encrypt and compress data for efficient and secure transmission to SEM
- Buffer events locally if you lose network connectivity to SEM

SEM provides access to the most frequently installed agents.

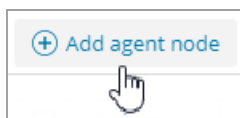
Install a Windows agent

Perform the following steps to install a Windows agent on a workstation.

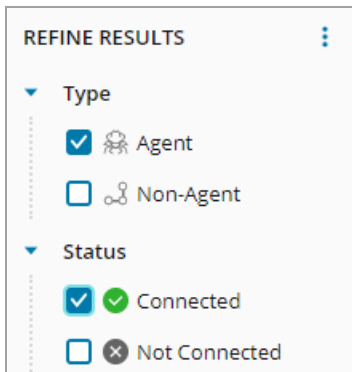
1. Review the [SEM agent pre-installation checklist](#).
2. [Log in to the SEM Console](#).
3. In the toolbar, click Configure > Nodes.



4. Click Add agent node.



5. Follow the on-screen instructions to install an agent.
 - a. Place the agent installation file (local installer or remote installer) on the local hard drive.
 - b. Right-click the installation file, and then select Run as administrator.
 - c. In the Manager Host field, enter the SEM IP address.
6. Verify that the SEM Manager is receiving agent data.
 - a. In the left column, select the Agent and Connected check boxes.



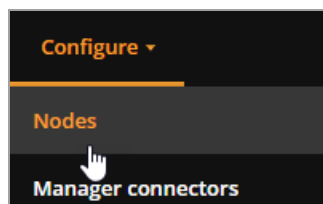
- b. In the center console, locate the targeted node and verify the connection status.



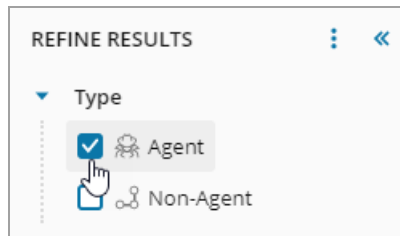
Configure the agent

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

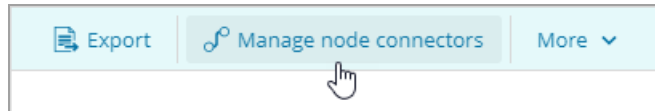
1. [Identify a SEM connector](#) for the targeted agent.
2. Log in to the SEM Console.
3. On the toolbar, click Configure > Nodes.



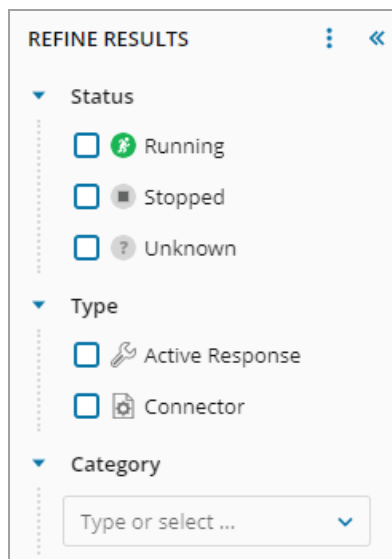
4. In the Refine Results column, expand Type and select the Agent checkbox.



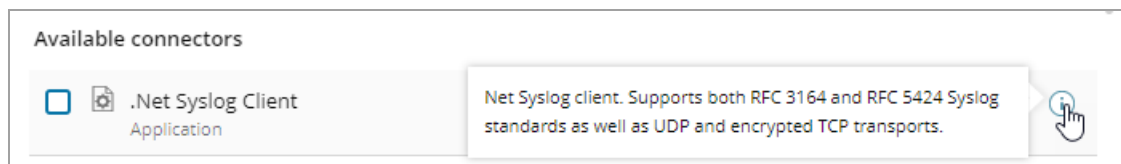
5. Select an agent, and then click Manage node connectors.



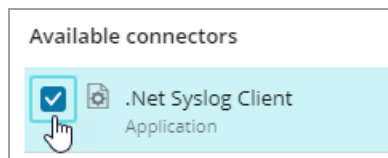
6. In the Refine Results column, sort the list of available connectors by status, type or category.



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.

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.

11. Under Sleep time, 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


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.

Add a syslog device to SEM

After you [configure your syslog device to send events to SEM](#) and [verify that SEM is receiving the events](#), add the syslog device to SEM.

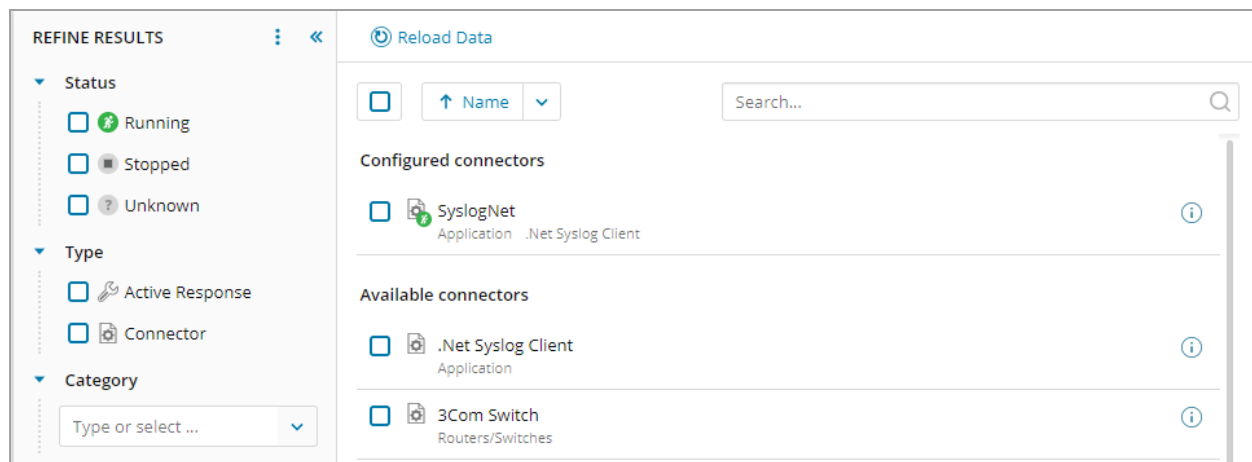
When you add a syslog device to SEM, select a connector that is specific to the network device you are adding. The connector normalizes the log data into a standard format that can be compared with logs received from other vendors' devices. See [SEM connectors](#) for a list of supported connectors.

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.

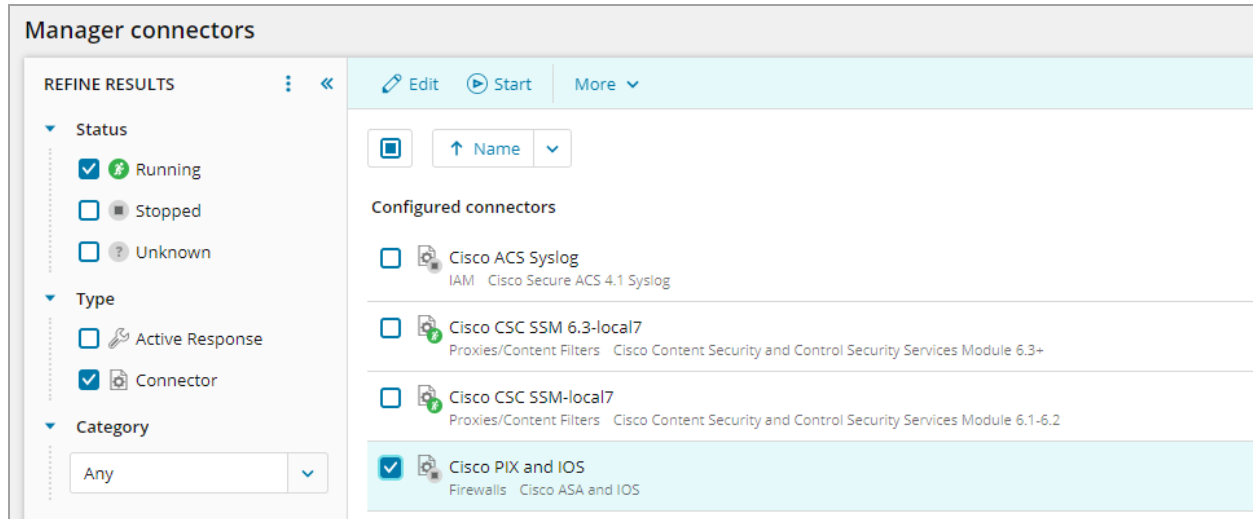


4. Select the connector, and then click Add Connector.
5. Complete the connector configuration form. The following fields are common across most connectors:
 - Name: Enter a user-friendly label for your connectors.

- 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.

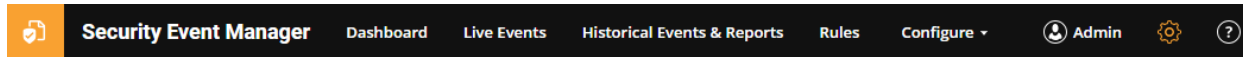


The screenshot displays the 'Manager connectors' interface in SolarWinds SEM. On the left, a 'REFINE RESULTS' sidebar allows filtering by Status (Running, Stopped, Unknown), Type (Active Response, Connector), and Category (Any). The main area shows a list of 'Configured connectors'. The 'Cisco PIX and IOS' connector is selected, indicated by a checkmark and a light blue background. Other connectors listed include 'Cisco ACS Syslog', 'Cisco CSC SSM 6.3-local7', and 'Cisco CSC SSM-local7'.

Connector Name	Status	Type	Category
Cisco ACS Syslog	Stopped	Connector	Any
Cisco CSC SSM 6.3-local7	Running	Connector	Any
Cisco CSC SSM-local7	Running	Connector	Any
Cisco PIX and IOS	Running	Connector	Any

Navigate the SEM Console

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

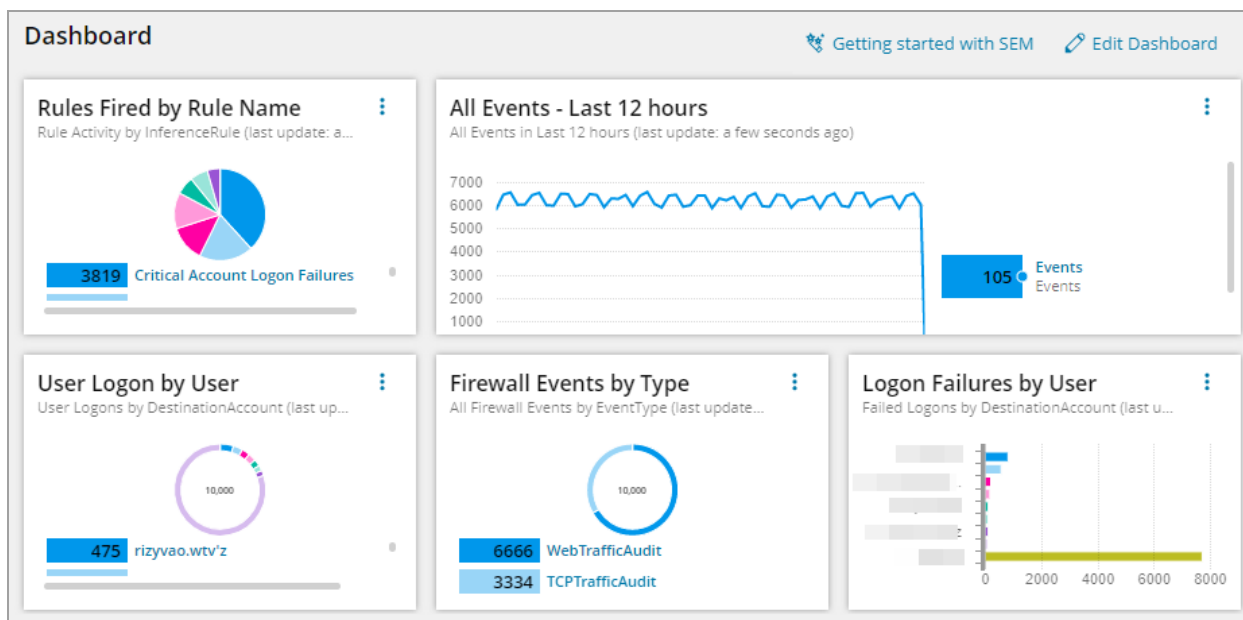


These views include:

- [Dashboard](#)
- [Live Events](#)
- [Historical Events & Reports](#)
- [Rules](#)
- [Nodes](#)
- [Configuration](#)
- [User-defined groups and email templates](#)

Dashboard

After you log in to the SEM Console, the SEM Dashboard (formerly SEM Ops Center) displays by default. Click Dashboard in the toolbar to access this view.

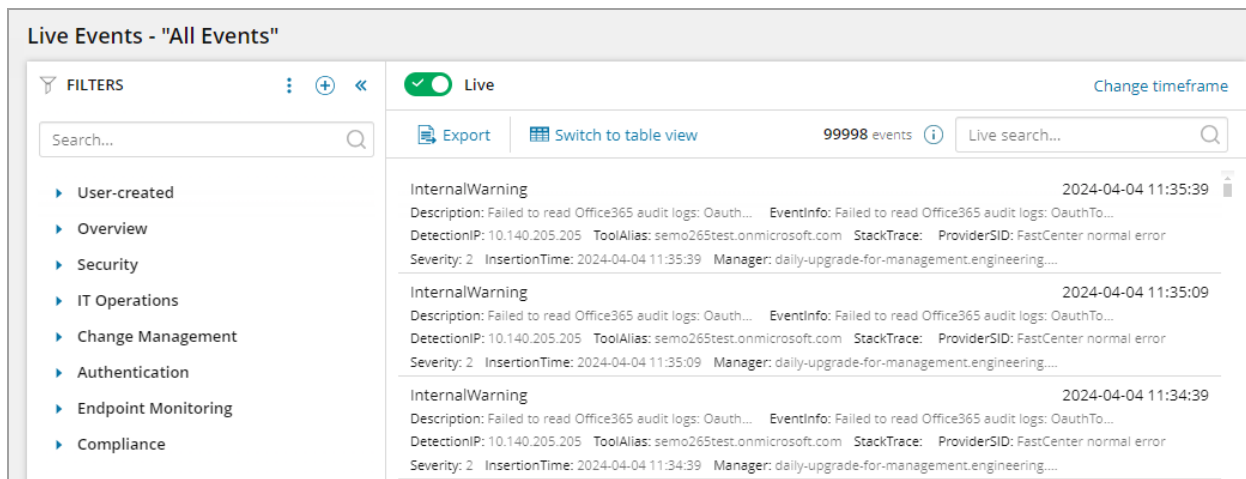


The dashboard allows you to visualize the network and log data in your corporate environment. Access the dashboard to highlight and summarize trends and suspicious activity through a series of interactive widgets. You can create, edit, and arrange widgets to display log data in a variety of tables and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

See [SEM Dashboard](#) in the SEM Administrator Guide for more information.

Live Events

The Live Events view provides instant access to live event monitoring for in-depth analysis and troubleshooting. Click Live Events in the toolbar to access this view. .



Live Events - "All Events"

FILTERS ⋮ + ⏪

Search...

- ▶ User-created
- ▶ Overview
- ▶ Security
- ▶ IT Operations
- ▶ Change Management
- ▶ Authentication
- ▶ Endpoint Monitoring
- ▶ Compliance

Live Change timeframe

Export **Switch to table view** **99998 events** Live search...

InternalWarning	2024-04-04 11:35:39
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 StackTrace: ProviderSID: FastCenter normal error	
Severity: 2 InsertionTime: 2024-04-04 11:35:39 Manager: daily-upgrade-for-management.engineering...	
InternalWarning	2024-04-04 11:35:09
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 StackTrace: ProviderSID: FastCenter normal error	
Severity: 2 InsertionTime: 2024-04-04 11:35:09 Manager: daily-upgrade-for-management.engineering...	
InternalWarning	2024-04-04 11:34:39
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 StackTrace: ProviderSID: FastCenter normal error	
Severity: 2 InsertionTime: 2024-04-04 11:34:39 Manager: daily-upgrade-for-management.engineering...	

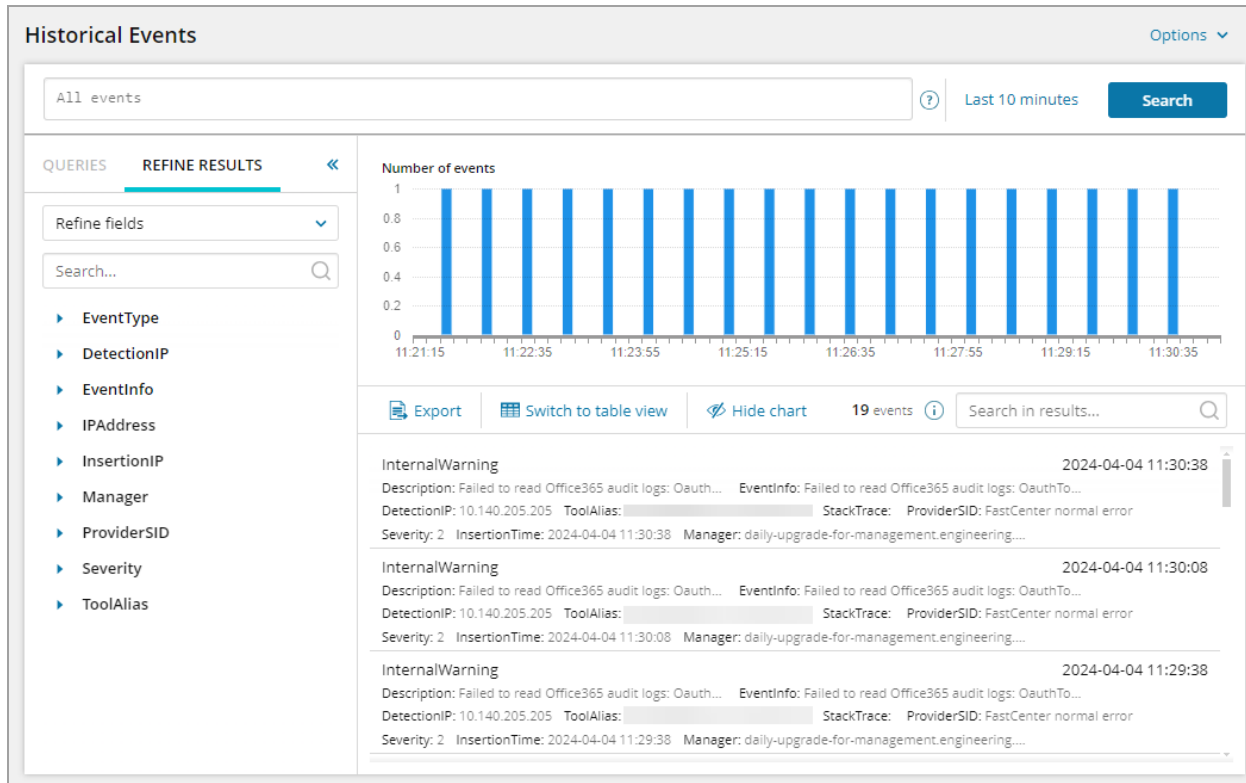
The Events table displays the events that exist for your selected filter. The title bar displays the name of the filter currently selected in the Filters pane. Events that match the selected filter are displayed as they occur if the Live Mode switch above the table is on. When set to off, the feed is frozen and the number of undisplayed event messages is displayed alongside the filter name.

The Filters pane displays the filters that can be applied to the event messages. To apply a filter, click to expand a filter group, and click on the filter. The events table title changes to the name of the filter and the table is refreshed to displays the incoming events matching the filter conditions.

See [Live Events view](#) in the SEM Administrator Guide for more information.

Historical Events & Reports

The Historical Events view displays any event data that passed through a particular SEM Manager instance. Click Historical Events & Reports to access this view.



You can use the historical data search to conduct custom searches, investigate your search results and event data, and then act on your findings. Additionally, you can switch between real-time event streaming and historical log views based on user-defined date and time parameters.

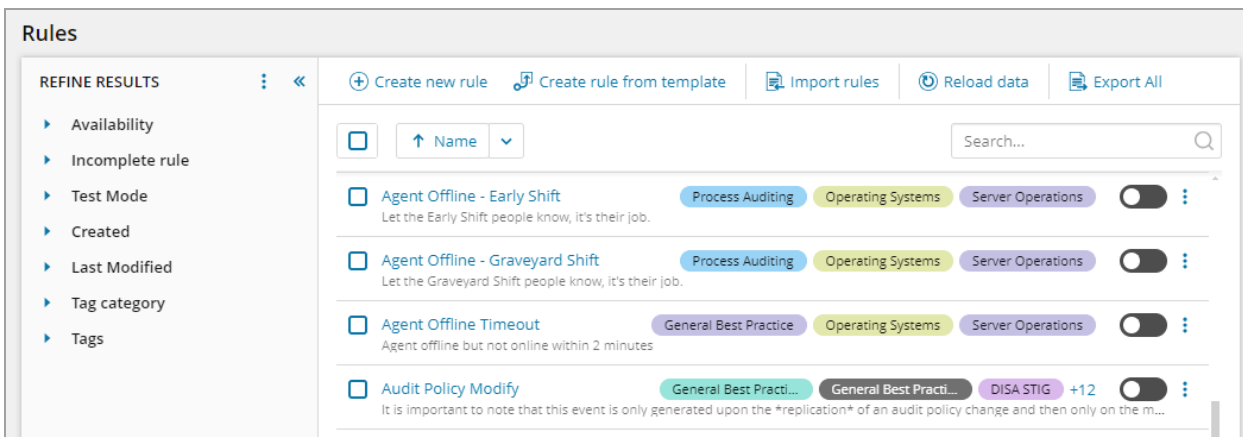
Click the Options drop-down menu to:

- Save and name a new query
- Generate a report in CSV or PDF format
- Save, name, and schedule a new query

See [Analyze Historical data](#) in the SEM Administrator Guide 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. Click Rules in the toolbar to access this view.

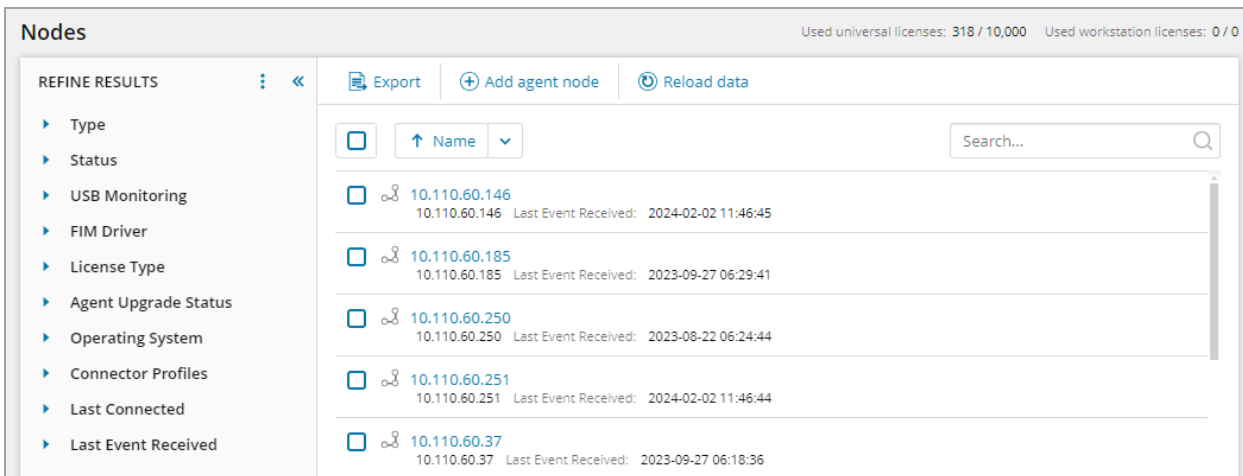


When an event (or a series of events) meets a rule condition, the rule prompts the SEM manager to act. A response action can be discreet (for example, sending a notification to select users by email), or active (for example, blocking an IP address or stopping a process).

See [Create rules that respond to security events](#) in the SEM Administrator Guide for more information.

Nodes

Through the HTML5-based node management feature, you can add agent nodes, configure connectors and connector profiles, and then monitor activity on the SEM Console. Click Configure > Nodes in the toolbar to access this view.



After you configure the node and connector, click the Events tab to view your network activity. When you are finished, 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 [Manage the monitored nodes](#) in the SEM Administrator Guide for more information.

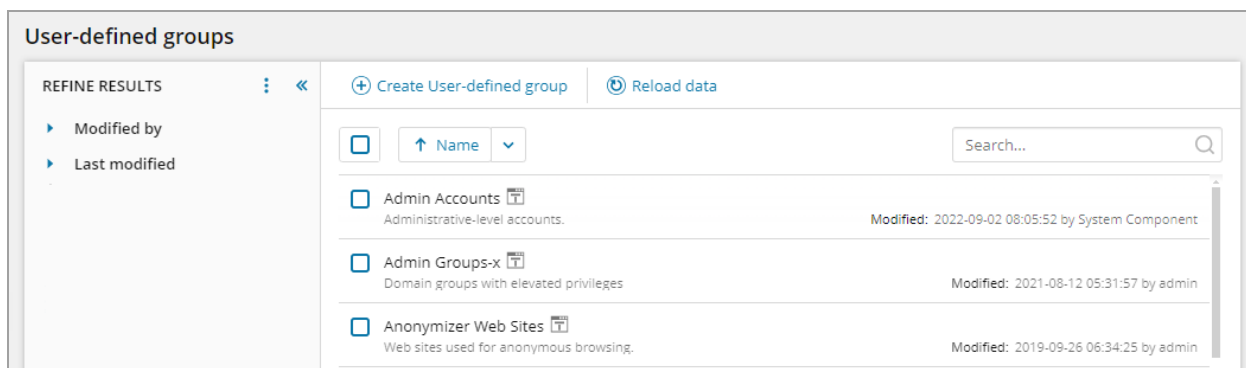
Configuration

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](#) in the SEM Administrator Guide for more information.

User-defined groups and email templates

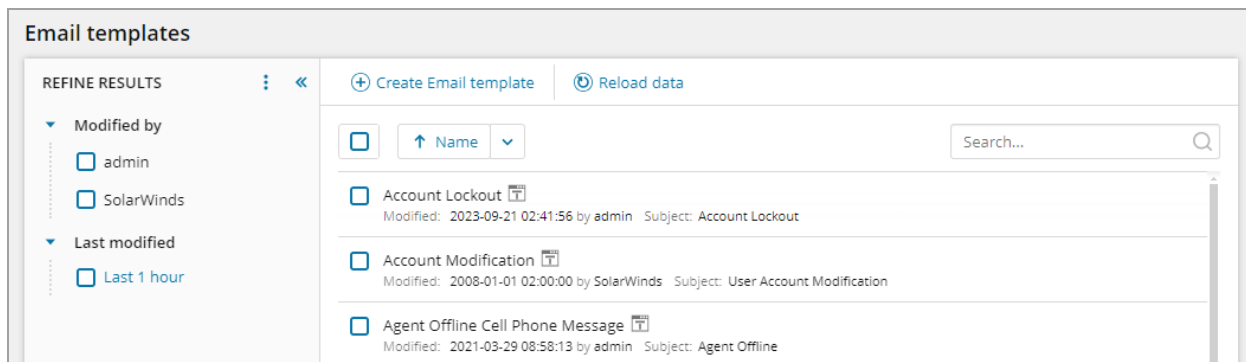
From the Groups tab, create user-defined groups to organize related elements for use with rules and filters. Click Configure > User defined groups in the toolbar to access this view.



Groups can contain elements such as events, IP addresses, computer names, and user accounts. After a group is defined, it can be referenced from multiple rules and filters.

See [Create user defined groups](#) in the SEM Administrator Guide for more information.

You can use email templates to customize your email notifications when triggered as responses in your custom rules. Click Configure > Email templates in the toolbar to access this view.



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.

See [Create email templates for use with SEM rules](#) in the SEM Administrator Guide for more information.

Beyond Getting Started with SEM

Now that you got started using SEM, see the [SEM Administrator Guide](#) to learn more about how to configure and set up SEM for your deployment.

For example, you can:

- [Secure your SEM deployment](#) to prevent access from unauthorized users
- [Configure the settings and services](#) to interact with the other systems and services in your IT environment
- [Create rules](#) that respond to security events in real time, whether or not you are monitoring the console
- [Manage the system resources](#) that SEM requires to work properly
- [Collect event data](#) from systems, devices, and applications in your network
- [View live and historical events](#) that occur in your network
- [Manage the monitored nodes](#) running with or without SEM agents
- [Monitor and protect specific systems and devices](#) in your network

You can also access the [SEM product forum](#) on [THWACK](#) to learn what's new in SEM and learn how other IT professionals are using the product.

SEM Getting Started: Additional Resources

Here are some additional resources to help you learn more about SolarWinds and how to get the most from SEM and other SolarWinds products.

- [New to SolarWinds products](#)
- [Virtual classrooms](#)
- [On-demand virtual classrooms](#)
- [SolarWinds onboarding programs](#)